

## LAB 3: DATA GATHERING AND FOOTPRINTING ON A TARGETED WEB SITE

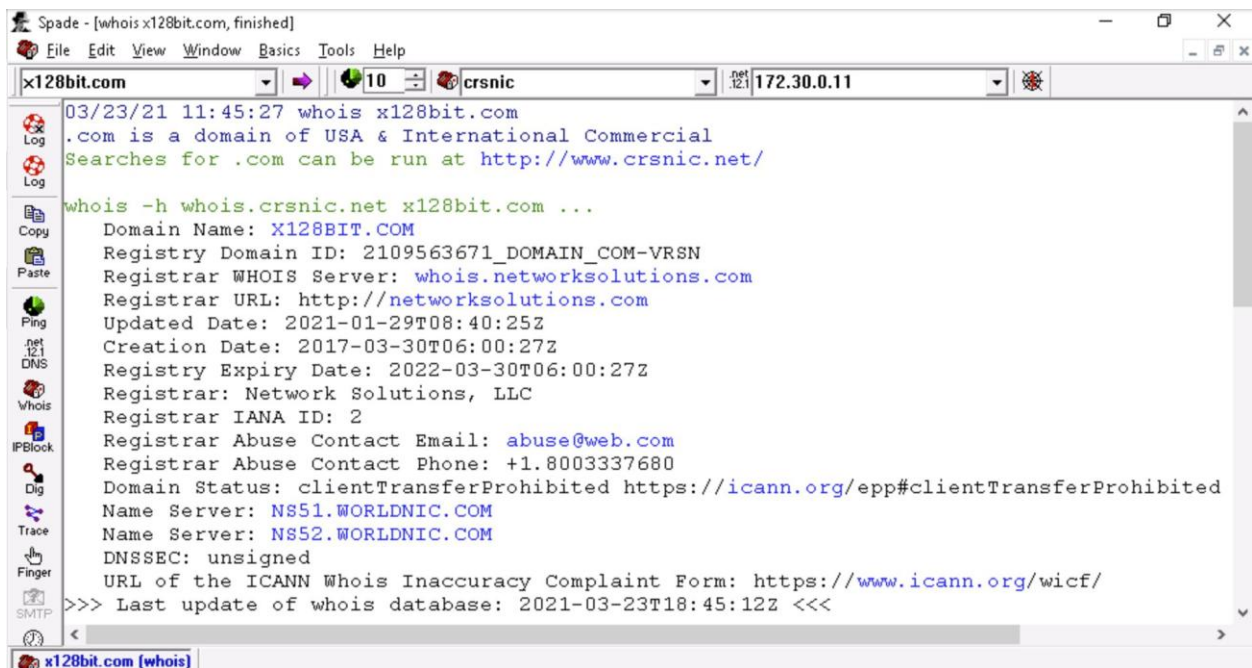
By: Jason Hodge

### Overview:

In this lab I used Sam Spade to do Whois searches and pings for x128bit.com, iSkytap.com, and Cloudparadox.com. I also conducted Nslookups and Traceroutes for these companies as well. Information gained in these searches could be extremely useful to any hacker in conducting many kinds of attacks.

### Section 1: Part 1:

Whois Searches and Pings for x128bit.com, iSkytap.com, and Cloudparadox.com



The screenshot shows the Sam Spade application window titled "Spade - [whois x128bit.com, finished]". The interface includes a menu bar (File, Edit, View, Window, Basics, Tools, Help) and a toolbar with icons for Log, Copy, Paste, Ping, net 121 DNS, Whois, IPBlock, Dig, Trace, Finger, and SMTP. The main window displays the results of a whois search for x128bit.com. The search was performed using the command "whois -h whois.crsnic.net x128bit.com ...". The results indicate that x128bit.com is a domain of USA & International Commercial, registered with Network Solutions, LLC. The domain status is clientTransferProhibited, and the name servers are NS51.WORLDDNIC.COM and NS52.WORLDDNIC.COM. The last update of the whois database was on 2021-03-23T18:45:12Z.

```
03/23/21 11:45:27 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: 2021-01-29T08:40:25Z
Creation Date: 2017-03-30T06:00:27Z
Registry Expiry Date: 2022-03-30T06:00:27Z
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: 2021-03-23T18:45:12Z <<<
```

Spade - [ping x128bit.com, finished]

File Edit View Window Basics Tools Help

x128bit.com 10 crsnic .net 172.30.0.11

```
03/23/21 11:49:04 ping x128bit.com
Ping x128bit.com (208.91.197.27) ...
 1 Addr:208.91.197.27, RTT: 48ms, TTL: 239
 2 Addr:208.91.197.27, RTT: 48ms, TTL: 239
 3 Addr:208.91.197.27, RTT: 48ms, TTL: 239
 4 Addr:208.91.197.27, RTT: 48ms, TTL: 239
 5 Addr:208.91.197.27, RTT: 48ms, TTL: 239
 6 Addr:208.91.197.27, RTT: 48ms, TTL: 239
 7 Addr:208.91.197.27, RTT: 48ms, TTL: 239
 8 Addr:208.91.197.27, RTT: 49ms, TTL: 239
 9 Addr:208.91.197.27, RTT: 49ms, TTL: 239
10 Addr:208.91.197.27, RTT: 48ms, TTL: 239
```

Spade - [whois iSkytap.com, finished]

File Edit View Window Basics Tools Help

iSkytap.com 10 crsnic .net 172.30.0.11

```
03/23/21 11:51:58 whois iskytap.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 iskytap.com ...
Domain Name: ISKYTAP.COM
Registry Domain ID: 2109563669_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.networksolutions.com
Registrar URL: http://networksolutions.com
Updated Date: 2021-01-29T08:40:24Z
Creation Date: 2017-03-30T06:00:27Z
Registry Expiry Date: 2022-03-30T06:00:27Z
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: NS45.WORLDDNIC.COM
Name Server: NS46.WORLDDNIC.COM
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2021-03-23T18:51:42Z <<<
```

iSkytap.com [whois]

Spade - [ping iSkytap.com, finished]

File Edit View Window Basics Tools Help

iSkytap.com 10 crsnic .net 172.30.0.11

```
03/23/21 11:53:32 ping iskytap.com
Ping iskytap.com (208.91.197.27) ...
 1 Addr:208.91.197.27, RTT: 49ms, TTL: 239
 2 Addr:208.91.197.27, RTT: 49ms, TTL: 239
 3 Addr:208.91.197.27, RTT: 49ms, TTL: 239
 4 Addr:208.91.197.27, RTT: 48ms, TTL: 239
 5 Addr:208.91.197.27, RTT: 49ms, TTL: 239
 6 Addr:208.91.197.27, RTT: 49ms, TTL: 239
 7 Addr:208.91.197.27, RTT: 48ms, TTL: 239
 8 Addr:208.91.197.27, RTT: 49ms, TTL: 239
 9 Addr:208.91.197.27, RTT: 48ms, TTL: 239
10 Addr:208.91.197.27, RTT: 48ms, TTL: 239
```

Spade - [whois Cloudparadox.com, finished]

File Edit View Window Basics Tools Help

Cloudparadox.com 10 crsnic 172.30.0.11

03/23/21 11:55:21 whois Cloudparadox.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 cloudparadox.com ...

Domain Name: CLOUDPARADOX.COM  
Registry Domain ID: 2109563670\_DOMAIN\_COM-VRSN  
Registrar WHOIS Server: [whois.networksolutions.com](http://whois.networksolutions.com)  
Registrar URL: <http://networksolutions.com>  
Updated Date: 2021-01-29T08:40:25Z  
Creation Date: 2017-03-30T06:00:27Z  
Registry Expiry Date: 2022-03-30T06:00:27Z  
Registrar: Network Solutions, LLC  
Registrar IANA ID: 2  
Registrar Abuse Contact Email: [abuse@web.com](mailto:abuse@web.com)  
Registrar Abuse Contact Phone: +1.8003337680  
Domain Status: clientTransferProhibited <https://icann.org/epp#clientTransferProhibited>  
Name Server: NS41.WORLDDNIC.COM  
Name Server: NS42.WORLDDNIC.COM  
DNSSEC: unsigned  
URL of the ICANN Whois Inaccuracy Complaint Form: <https://www.icann.org/wicf/>  
>>> Last update of whois database: 2021-03-23T18:55:13Z <<<

Cloudparadox.com

Spade - [ping Cloudparadox.com, finished]

File Edit View Window Basics Tools Help

Cloudparadox.com 10 crsnic 172.30.0.11

03/23/21 11:56:43 ping Cloudparadox.com

Ping Cloudparadox.com (206.188.192.97) ...

Seq	Addr	RTT	TTL
1	Addr:206.188.192.97	RTT: 29ms	TTL: 49
2	Addr:206.188.192.97	RTT: 28ms	TTL: 49
3	Addr:206.188.192.97	RTT: 28ms	TTL: 49
4	Addr:206.188.192.97	RTT: 28ms	TTL: 49
5	Addr:206.188.192.97	RTT: 29ms	TTL: 49
6	Addr:206.188.192.97	RTT: 28ms	TTL: 49
7	Addr:206.188.192.97	RTT: 28ms	TTL: 49
8	Addr:206.188.192.97	RTT: 29ms	TTL: 49
9	Addr:206.188.192.97	RTT: 29ms	TTL: 49
10	Addr:206.188.192.97	RTT: 29ms	TTL: 49

## Nslookup Information for x128bit.com, iSkytap.com, and Cloudparadox.com

```
Administrator: Command Prompt - nslookup
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>nslookup
Default Server:  dns.google
Address:  8.8.8.8

> set type=any
> x128bit.com
Server:  dns.google
Address:  8.8.8.8

Non-authoritative answer:
x128bit.com      nameserver = ns51.worldnic.com
x128bit.com      internet address = 208.91.197.27
x128bit.com
    primary name server = ns51.worldnic.com
    responsible mail addr = namehost.worldnic.com
    serial = 120071403
    refresh = 10800 (3 hours)
    retry = 3600 (1 hour)
    expire = 604800 (7 days)
    default TTL = 3600 (1 hour)
x128bit.com      MX preference = 10, mail exchanger = mx1.netsolmail.net
x128bit.com      nameserver = ns52.worldnic.com
> _
```

```
> iSkytap.com
Server:  dns.google
Address:  8.8.8.8

Non-authoritative answer:
iSkytap.com      internet address = 208.91.197.27
iSkytap.com      nameserver = ns45.worldnic.com
iSkytap.com
    primary name server = ns45.worldnic.com
    responsible mail addr = namehost.worldnic.com
    serial = 120071322
    refresh = 10800 (3 hours)
    retry = 3600 (1 hour)
    expire = 604800 (7 days)
    default TTL = 3600 (1 hour)
iSkytap.com      nameserver = ns46.worldnic.com
> _
```

```

> Cloudparadox.com
Server: dns.google
Address: 8.8.8.8

Non-authoritative answer:
Cloudparadox.com      nameserver = ns42.worldnic.com
Cloudparadox.com
    primary name server = NS41.worldnic.com
    responsible mail addr = namehost.worldnic.com
    serial = 121020918
    refresh = 10800 (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 = 206.188.192.97
> _

```

Traceroute information for x128bit.com, iSkytap.com, and Cloudparadox.com

```

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

  1  <1 ms  <1 ms  <1 ms  192.168.109.254
  2   1 ms   <1 ms  <1 ms  172.18.249.251
  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  66.79.244.225
  6   8 ms   1 ms   <1 ms  v705.core1.tor1.he.net [216.66.14.249]
  7  10 ms  10 ms  10 ms  100ge14-2.core1.nyc4.he.net [184.105.80.9]
  8  76 ms  79 ms  76 ms  100ge7-1.core1.lon2.he.net [72.52.92.165]
  9  82 ms  82 ms  82 ms  100ge6-2.core1.ams1.he.net [72.52.92.214]
 10   *      *      *      Request timed out.
 11   *      *      *      Request timed out.
 12   *      *      *      Request timed out.
 13   *      *      *      Request timed out.
 14   *      *      *      Request timed out.
 15 115 ms 134 ms 114 ms  ae1.mpr1.aus1.us.zip.zayo.com [64.125.27.30]
 16 115 ms 114 ms 114 ms  ae3.er1.aus3.us.zip.zayo.com [64.125.31.25]
 17 114 ms 114 ms 115 ms  209.66.92.122.IPYX-085258-900-ZYO.above.net [209.66.92.122]
 18 115 ms 115 ms 115 ms  po10.gw2.pod1.tx1.datafoundry.net [209.99.14.106]
 19 115 ms 115 ms 115 ms  206-127-10-90.fwd.datafoundry.com [206.127.10.90]
 20 115 ms 114 ms 114 ms  po60.colo3.aus1.datafoundry.net [207.207.35.194]
 21   *      *      123 ms  209-99-48-54.fwd.datafoundry.com [209.99.48.54]
 22 123 ms 123 ms 122 ms  208.91.197.27

Trace complete.

```



```
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	192.168.109.254
2	1 ms	<1 ms	<1 ms	172.18.249.251
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	66.79.244.225
6	1 ms	<1 ms	<1 ms	v705.core1.tor1.he.net [216.66.14.249]
7	11 ms	10 ms	11 ms	100ge14-2.core1.nyc4.he.net [184.105.80.9]
8	76 ms	76 ms	76 ms	100ge7-1.core1.lon2.he.net [72.52.92.165]
9	*	*	*	Request timed out.
10	*	*	*	Request timed out.
11	*	*	*	Request timed out.
12	*	*	115 ms	ae23.cs3.iad93.us.eth.zayo.com [64.125.28.189]
13	*	*	*	Request timed out.
14	48 ms	48 ms	49 ms	ae3.er1.aus3.us.zip.zayo.com [64.125.31.25]
15	*	*	*	Request timed out.
16	*	*	*	Request timed out.
17	*	*	*	Request timed out.
18	*	*	*	Request timed out.
19	*	*	*	Request timed out.
20	*	*	*	Request timed out.
21	*	*	*	Request timed out.
22	*	*	63 ms	208.91.197.27

```
Trace complete.
```

```
C:\Users\Administrator>tracert Cloudparadox.com
```

```
Tracing route to Cloudparadox.com [206.188.192.97]  
over a maximum of 30 hops:
```

1	<1 ms	<1 ms	<1 ms	192.168.109.254
2	1 ms	<1 ms	<1 ms	172.18.249.251
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	66.79.244.225
6	1 ms	1 ms	1 ms	cloudflare.ip4.torontointernetexchange.net [206.108.34.208]
7	<1 ms	<1 ms	<1 ms	108.162.240.191
8	1 ms	<1 ms	<1 ms	108.162.240.30
9	*	*	*	Request timed out.
10	28 ms	33 ms	28 ms	209.17.112.42
11	28 ms	28 ms	28 ms	vux.netsolhost.com [206.188.192.97]
12	29 ms	28 ms	30 ms	vux.netsolhost.com [206.188.192.97]

```
Trace complete.
```

## **Part 2:**

Name of Target Organization: Amazon

Domain Name and Extension: Amazon.com

URL: <https://www.amazon.com/>

Physical Address Info: Amazon corporate offices located at 410 Terry Ave. North, Seattle, WA, 98109-5210; phone (206) 266-1000.

President, CEO, Chairman of the Board: Jeffrey P. Bezos

Senior Vice President and Chief Financial Officer: Brian T. Olsavsky

CEO Worldwide Consumer: David H. Clark

Chief Executive Officer, Amazon Web Services: Andrew R. Jassy

Vice President, Worldwide Controller: Shelley L. Reynolds

Senior Vice President, General Counsel and Secretary: David A. Zapolsky  
Recently topped 75,000 employees in Seattle Area.

Business Partners: 3M, Intel, Vari, etc.

## **Part 3:**

### **Executive Summary:**

The information gained in Part 1 regarding Whois, Nslookup, and Traceroute data, are extremely useful to hackers. The Whois record contains all contact information including the person, group, or company that registered a domain name, this includes dates, names of servers, and expiration dates. This information can be used for fraud attacks such as domain hijacking and phishing, registrar hacking, as well as DNS attacks and cache poisoning.

In an Nslookup I gained information about x128bit.com, iSkytap.com, and Cloudparadox.com to find the name of the server, internet address, serial number, expiration date, etc. I also used the tracert command in command prompt to track the real time pathway taken by packets hopping from router to router with the IP addresses and time taken for each hop.

In Part 2, information pertaining to Amazon.com was plentiful. Lots of valuable data regarding addresses, phone numbers, employees, and positions, as well as business partners were found.

**Methodology:** In this lab I used Sam Spade to look up Whois information and send a ping for x128bit.com, iSkytap.com, and Cloudparadox.com. Then I did a nslookup in command prompt to find the name of the server, internet address, serial number, expiration date, etc. Lastly, the tracert command was used in command prompt to track the real time pathway taken by packets hopping from router to router with the IP addresses and time taken for each hop. The target organization chosen was Amazon.com. Using just google I was able to find lots of valuable information regarding addresses, phone numbers, employees, and positions, as well as business partners.

**Technical Research Results:** In Part 1 the technical research found included Whois and ping information for x128bit.com, iSkytap.com, and Cloudparadox.com. Also included was information found in nslookups and traceroutes for the three companies. Information provided in these methods are included in the methodology.

**Public Domain Research Results:** In Part 2 public domain research found regarding the target company Amazon was plentiful. Lots of valuable data regarding addresses, phone numbers, employees, and positions, as well as business partners were found.

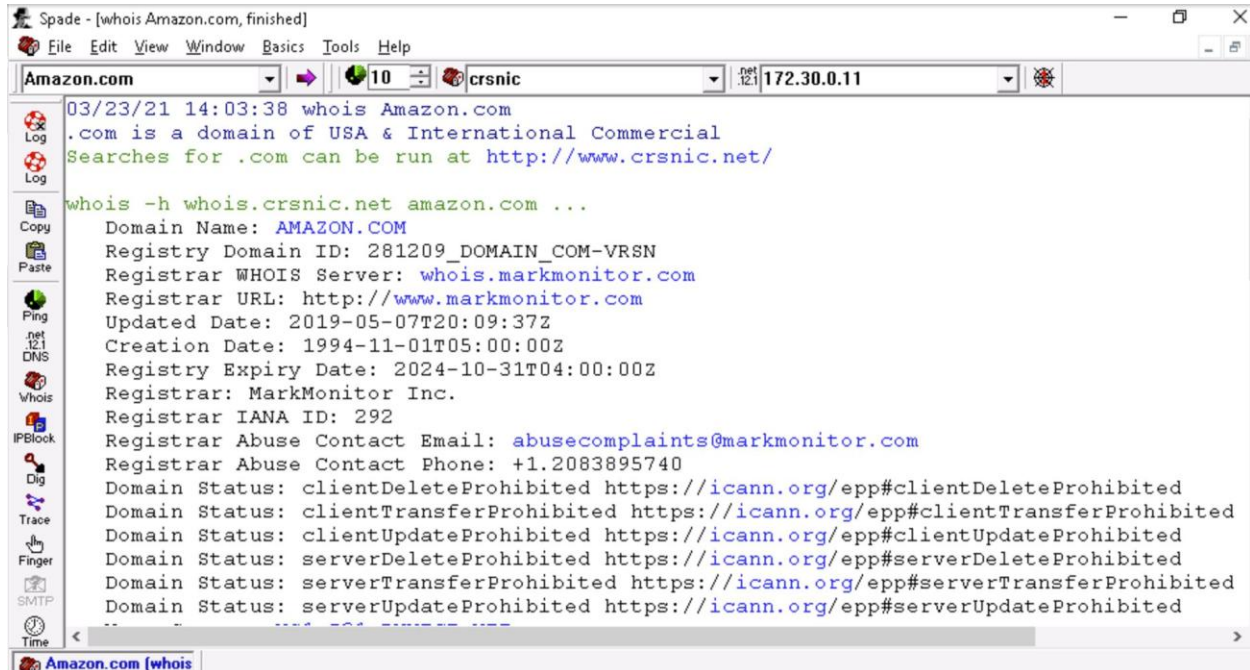
**Findings and Conclusions:** Lots of useful information was found about x128bit.com, iSkytap.com, Cloudparadox.com, and Amazon.com through using the tools in this lab. Information gained can be used for varieties of attacks on these companies and this data was not hard to find. This data can be used for fraud attacks such as domain hijacking and phishing, registrar hacking, as well as DNS attacks such as DNS spoofing, DNS amplification, DDoS and cache poisoning. This information can also be used for DNS queries to conduct SQL injection attacks, as well as man in the middle attacks such as session hijacking and IP spoofing.

**Avenues of Further Research:** Additional research that would prove to be useful would include information needed for different types of attacks not mentioned above. Attacks not mentioned include TCP SYN flooding attacks, teardrop attacks, botnet attacks, and others. These attacks can all be conducted through information regarding firewalls, TCP data, as well as network and bandwidth information.



## Section 2 Part 1 (Part 2 and 3 are Included in Report Above):

### Whois Sam Spade Search and Ping for Amazon.com



Spade - [whois Amazon.com, finished]

File Edit View Window Basics Tools Help

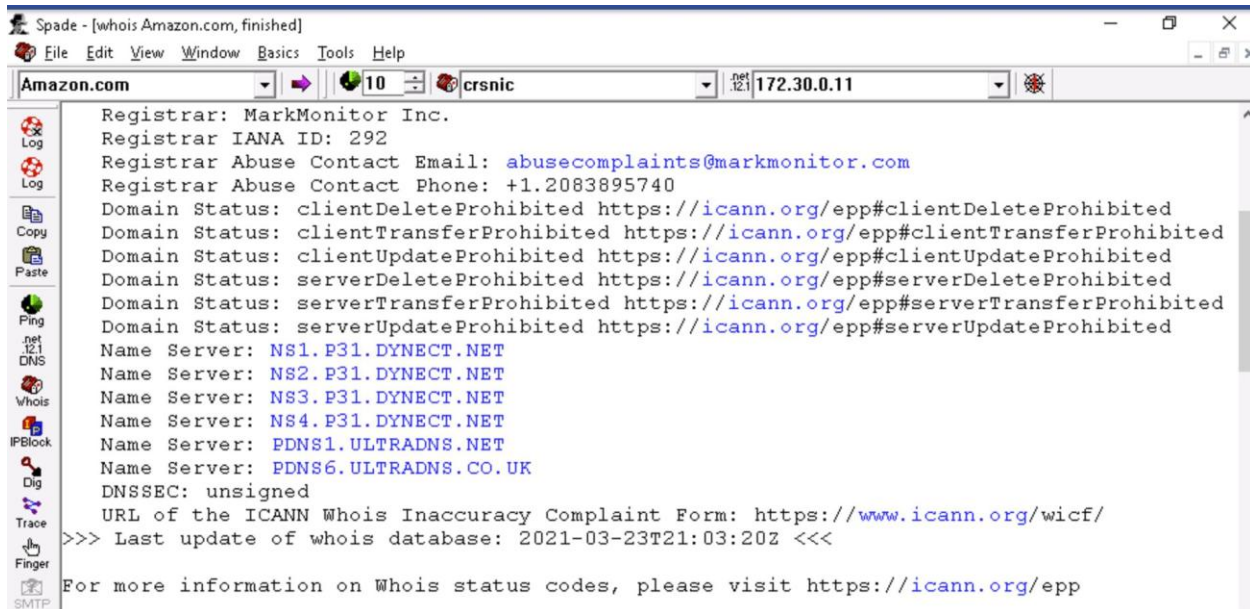
Amazon.com 10 crsnic 172.30.0.11

03/23/21 14:03:38 whois Amazon.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 amazon.com ...

Domain Name: **AMAZON.COM**  
Registry Domain ID: 281209\_DOMAIN\_COM-VRSN  
Registrar WHOIS Server: [whois.markmonitor.com](http://whois.markmonitor.com)  
Registrar URL: <http://www.markmonitor.com>  
Updated Date: 2019-05-07T20:09:37Z  
Creation Date: 1994-11-01T05:00:00Z  
Registry Expiry Date: 2024-10-31T04:00:00Z  
Registrar: MarkMonitor Inc.  
Registrar IANA ID: 292  
Registrar Abuse Contact Email: [abusecomplaints@markmonitor.com](mailto:abusecomplaints@markmonitor.com)  
Registrar Abuse Contact Phone: +1.2083895740  
Domain Status: clientDeleteProhibited <https://icann.org/epp#clientDeleteProhibited>  
Domain Status: clientTransferProhibited <https://icann.org/epp#clientTransferProhibited>  
Domain Status: clientUpdateProhibited <https://icann.org/epp#clientUpdateProhibited>  
Domain Status: serverDeleteProhibited <https://icann.org/epp#serverDeleteProhibited>  
Domain Status: serverTransferProhibited <https://icann.org/epp#serverTransferProhibited>  
Domain Status: serverUpdateProhibited <https://icann.org/epp#serverUpdateProhibited>

Amazon.com [whois]

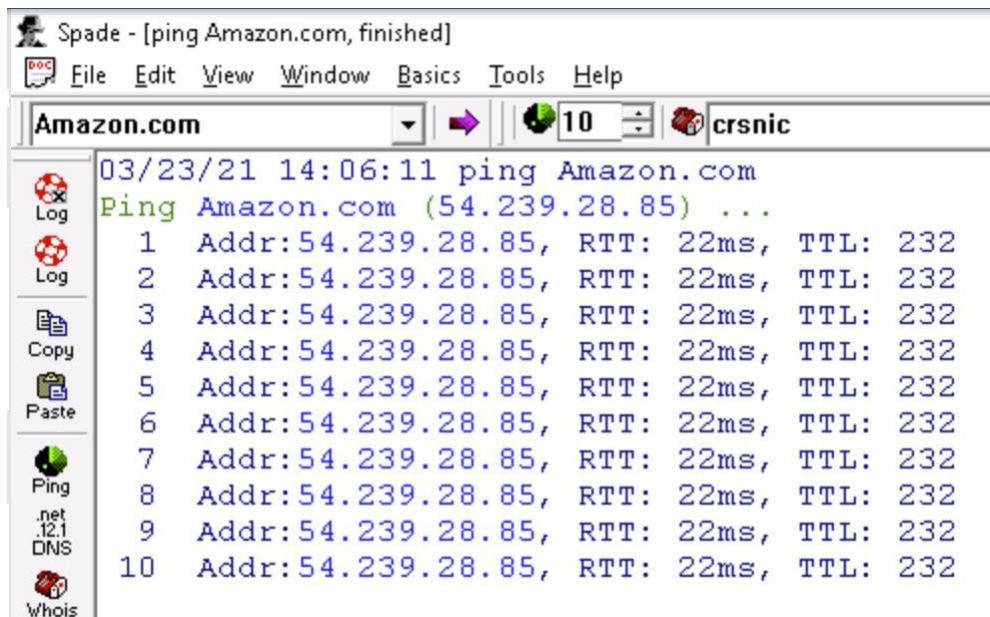


Spade - [whois Amazon.com, finished]

File Edit View Window Basics Tools Help

Amazon.com 10 crsnic 172.30.0.11

Registrar: MarkMonitor Inc.  
Registrar IANA ID: 292  
Registrar Abuse Contact Email: [abusecomplaints@markmonitor.com](mailto:abusecomplaints@markmonitor.com)  
Registrar Abuse Contact Phone: +1.2083895740  
Domain Status: clientDeleteProhibited <https://icann.org/epp#clientDeleteProhibited>  
Domain Status: clientTransferProhibited <https://icann.org/epp#clientTransferProhibited>  
Domain Status: clientUpdateProhibited <https://icann.org/epp#clientUpdateProhibited>  
Domain Status: serverDeleteProhibited <https://icann.org/epp#serverDeleteProhibited>  
Domain Status: serverTransferProhibited <https://icann.org/epp#serverTransferProhibited>  
Domain Status: serverUpdateProhibited <https://icann.org/epp#serverUpdateProhibited>  
Name Server: **NS1.P31.DYNECT.NET**  
Name Server: **NS2.P31.DYNECT.NET**  
Name Server: **NS3.P31.DYNECT.NET**  
Name Server: **NS4.P31.DYNECT.NET**  
Name Server: **PDNS1.ULTRADNS.NET**  
Name Server: **PDNS6.ULTRADNS.CO.UK**  
DNSSEC: unsigned  
URL of the ICANN Whois Inaccuracy Complaint Form: <https://www.icann.org/wicf/>  
>>> Last update of whois database: 2021-03-23T21:03:20Z <<<  
For more information on Whois status codes, please visit <https://icann.org/epp>



## Whois Command Prompt Search for Amazon.com

```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>whois Amazon.com

WHOIS Server: whois.markmonitor.com

Domain Name: amazon.com
Registry Domain ID: 281209_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.markmonitor.com
Registrar URL: http://www.markmonitor.com
Updated Date: 2019-08-26T12:19:56-0700
Creation Date: 1994-10-31T21:00:00-0800
Registrar Registration Expiration Date: 2024-10-30T00:00:00-0700
Registrar: MarkMonitor, Inc.
Registrar IANA ID: 292
Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
Registrar Abuse Contact Phone: +1.2083895770
Domain Status: clientUpdateProhibited (https://www.icann.org/epp#clientUpdateProhibited)
Domain Status: clientTransferProhibited (https://www.icann.org/epp#clientTransferProhibited)
Domain Status: clientDeleteProhibited (https://www.icann.org/epp#clientDeleteProhibited)
Domain Status: serverUpdateProhibited (https://www.icann.org/epp#serverUpdateProhibited)
Domain Status: serverTransferProhibited (https://www.icann.org/epp#serverTransferProhibited)
Domain Status: serverDeleteProhibited (https://www.icann.org/epp#serverDeleteProhibited)
Registry Registrant ID:
Registrant Name: Hostmaster, Amazon Legal Dept.
Registrant Organization: Amazon Technologies, Inc.
Registrant Street: P.O. Box 8102
Registrant City: Reno
Registrant State/Province: NV
Registrant Postal Code: 89507
```

Registrant Country: US  
Registrant Phone: +1.2062664064  
Registrant Phone Ext:  
Registrant Fax: +1.2062667010  
Registrant Fax Ext:  
Registrant Email: hostmaster@amazon.com  
Registry Admin ID:  
Admin Name: Hostmaster, Amazon Legal Dept.  
Admin Organization: Amazon Technologies, Inc.  
Admin Street: P.O. Box 8102  
Admin City: Reno  
Admin State/Province: NV  
Admin Postal Code: 89507  
Admin Country: US  
Admin Phone: +1.2062664064  
Admin Phone Ext:  
Admin Fax: +1.2062667010  
Admin Fax Ext:  
Admin Email: hostmaster@amazon.com  
Registry Tech ID:  
Tech Name: Hostmaster, Amazon Legal Dept.  
Tech Organization: Amazon Technologies, Inc.  
Tech Street: P.O. Box 8102  
Tech City: Reno  
Tech State/Province: NV  
Tech Postal Code: 89507  
Tech Country: US  
Tech Phone: +1.2062664064  
Tech Phone Ext:  
Tech Fax: +1.2062667010  
Tech Fax Ext:

Tech Fax: +1.2062667010  
Tech Fax Ext:  
Tech Email: hostmaster@amazon.com  
Name Server: ns3.p31.dynect.net  
Name Server: pdns6.ultradns.co.uk  
Name Server: ns4.p31.dynect.net  
Name Server: ns2.p31.dynect.net  
Name Server: ns1.p31.dynect.net  
Name Server: pdns1.ultradns.net  
DNSSEC: unsigned  
URL of the ICANN WHOIS Data Problem Reporting System: <http://wdprs.internic.net/>  
>>> Last update of WHOIS database: 2021-03-23T14:59:25-0700 <<<  
  
For more information on WHOIS status codes, please visit:  
<https://www.icann.org/resources/pages/epp-status-codes>

## Fast Traceroute Sam Spade for Amazon.com

03/23/21 15:09:36 Fast traceroute Amazon.com

Trace Amazon.com (205.251.242.103) ...

Hop	IP Address	Time	TTL	Notes
1	192.168.108.254	0ms	0ms	TTL: 64 (No rDNS)
2	172.18.249.250	0ms	1ms	TTL: 254 (No rDNS)
3	172.18.0.2	0ms	0ms	TTL: 62 (No rDNS)
4	76.75.74.129	0ms	0ms	TTL: 252 (No rDNS)
5	66.79.244.225	0ms	0ms	TTL: 250 (No rDNS)
6	206.108.35.37	0ms	0ms	TTL: 249 (amazon-b.ip4.torontointernetexchange.net)
7	No Response	*	*	*
8	No Response	*	*	*
9	150.222.79.79	1ms	1ms	0ms TTL: 245 (No rDNS)
10	52.93.3.111	0ms	0ms	0ms TTL: 247 (No rDNS)
11	No Response	*	*	*
12	No Response	*	*	*
13	No Response	*	*	*
14	No Response	*	*	*
15	No Response	*	*	*
16	52.93.28.222	22ms	22ms	22ms TTL: 242 (No rDNS)
17	No Response	*	*	*
18	No Response	*	*	*
19	No Response	*	*	*
20	No Response	*	*	*
21	No Response	*	*	*
22	No Response	*	*	*
23	No Response	*	*	*
24	No Response	*	*	*
25	No Response	*	*	*
26	No Response	*	*	*
27	No Response	*	*	*
28	72.21.218.197	23ms	23ms	23ms TTL: 234 (No rDNS)
29	205.251.242.103	22ms	22ms	22ms TTL: 233 (s3-console-us-standard.console.aws.ama)

## Traceroute Command Prompt for Amazon.com

```
C:\Users\Administrator>tracert Amazon.com

Tracing route to Amazon.com [205.251.242.103]
over a maximum of 30 hops:

  1  <1 ms    <1 ms    <1 ms    192.168.108.254
  2  <1 ms    <1 ms    <1 ms    172.18.249.250
  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    66.79.244.225
  6  1 ms     <1 ms    <1 ms    amazon-b.ip4.torontointernetwork.net [206.108.35.37]
  7  *         *         *         Request timed out.
  8  *         *         *         Request timed out.
  9  1 ms     1 ms     1 ms     150.222.79.79
 10 <1 ms    <1 ms    <1 ms    52.93.3.111
 11 *         *         *         Request timed out.
 12 *         *         *         Request timed out.
 13 *         *         *         Request timed out.
 14 *         *         *         Request timed out.
 15 *         *         *         Request timed out.
 16 22 ms    22 ms    22 ms    52.93.28.222
 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 23 ms    23 ms    23 ms    72.21.218.197
 29 22 ms    22 ms    21 ms    s3-console-us-standard.console.aws.amazon.com [205.251.242.103]

Trace complete.
```



## Sam Spade Dig for Amazon.com

Spade - [dig Amazon.com @ 172.30.0.11, finished]

File Edit View Window Basics Tools Help

Amazon.com 10 crsnic .net 172.30.0.11

03/23/21 15:25:58 dig Amazon.com @ 172.30.0.11  
Dig Amazon.com@ns3.p31.dynect.net (208.78.71.31) ...  
Authoritative Answer  
Query for Amazon.com type=255 class=1  
amazon.com SOA (Zone of Authority)  
Primary NS: dns-external-master.Amazon.com  
Responsible person: root@Amazon.com  
serial:2010131665  
refresh:180s (3 minutes)  
retry:60s  
expire:3024000s (35 days)  
minimum-ttl:60s  
Amazon.com NS (Nameserver) pdns6.ultradns.co.uk  
Amazon.com NS (Nameserver) ns1.p31.dynect.net  
Amazon.com NS (Nameserver) ns4.p31.dynect.net  
Amazon.com NS (Nameserver) ns2.p31.dynect.net  
Amazon.com NS (Nameserver) ns3.p31.dynect.net  
Amazon.com NS (Nameserver) pdns1.ultradns.net  
Amazon.com A (Address) 176.32.103.205  
Amazon.com A (Address) 205.251.242.103  
Amazon.com A (Address) 54.239.28.85  
Amazon.com MX (Mail Exchanger) Priority: 5 amazon-smtp.Amazon.com

Amazon.com MX (Mail Exchanger) Priority: 5 amazon-smtp.Amazon.com  
Amazon.com TXT (Text Field)  
v=spf1 include:spf1.amazon.com include:spf2.amazon.com include:amazonses.com -all  
pywpmqÀ qqE0OwwHqOq0HKhb7rDQÀ Amazon.com TXT (Text Field)  
wrike-verification=MzI3NzM2ODo2NDk5MjE4NjQ2MmWJmOTewMGMxM2MzNzJmNWJlY2U5ZDU4MmVlNzQ2NWU  
wwHqOq0HKhb7rDQÀ Amazon.com TXT (Text Field)  
facebook-domain-verification=d9u57u52gylohx845ogolaxzpywpmq  
Amazon.com TXT (Text Field)  
MS=4B600B22799EB2CAC0D8FF0A3A3CAECA5EE2BF3A  
Amazon.com TXT (Text Field)  
google-site-verification=14WGW2MdNMxchG8PlinF7LgqqE0OwwHqOq0HKhb7rDQ  
Amazon.com TXT (Text Field)  
spf2.0/pra include:spf1.amazon.com include:spf2.amazon.com include:amazonses.com -all  
Dig Amazon.com@ns2.p31.dynect.net (204.13.250.31) ...  
Authoritative Answer  
Query for Amazon.com type=255 class=1  
amazon.com SOA (Zone of Authority)  
Primary NS: dns-external-master.Amazon.com  
Responsible person: root@Amazon.com  
serial:2010131665  
refresh:180s (3 minutes)  
retry:60s



```
retry:60s
expire:3024000s (35 days)
minimum-ttl:60s
Amazon.com NS (Nameserver) ns4.p31.dynect.net
Amazon.com NS (Nameserver) pdns1.ultradns.net
Amazon.com NS (Nameserver) pdns6.ultradns.co.uk
Amazon.com NS (Nameserver) ns1.p31.dynect.net
Amazon.com NS (Nameserver) ns3.p31.dynect.net
Amazon.com NS (Nameserver) ns2.p31.dynect.net
Amazon.com A (Address) 205.251.242.103
Amazon.com A (Address) 54.239.28.85
Amazon.com A (Address) 176.32.103.205
Amazon.com MX (Mail Exchanger) Priority: 5 amazon-smtp.Amazon.com
Amazon.com TXT (Text Field)
v=spf1 include:spf1.amazon.com include:spf2.amazon.com include:amazonses.com -all
  00B22799EB2CAC0D8FF0A3A3CAECA5EE2BF3A
spf2.0/prd include:spf1.amazon.com include:spf2.amazon.com include:amazonses.com -all
  Amazon.com TXT (Text Field)
wrike-verification=MzI3NzM2ODo2NDk5MjE4NjQ2MmWJmOTewMGMxM2MzNzJmNWJlY2U5ZDU4MmVlNzQ2NWU
  Amazon.com TXT (Text Field)
MS=4B600B22799EB2CAC0D8FF0A3A3CAECA5EE2BF3A
Amazon.com TXT (Text Field)
```

```
Amazon.com TXT (Text Field)
google-site-verification=14WGW2MdNMxchG8PlinF7LgqqE0OwwHqOq0HKhb7rDQ
Amazon.com TXT (Text Field)
facebook-domain-verification=d9u57u52gylohx845ogolaxzpywpmq
Dig Amazon.com@pdns1.ultradns.net (204.74.108.1) ...
Authoritative Answer
Query for Amazon.com type=255 class=1
amazon.com HINFO (Host Info) Cpu:RFC8482 Os:
amazon.com NS (Nameserver) pdns1.ultradns.net
amazon.com NS (Nameserver) ns4.p31.dynect.net
amazon.com NS (Nameserver) ns3.p31.dynect.net
amazon.com NS (Nameserver) ns2.p31.dynect.net
amazon.com NS (Nameserver) ns1.p31.dynect.net
amazon.com NS (Nameserver) pdns6.ultradns.co.uk
Dig Amazon.com@pdns6.ultradns.co.uk (204.74.115.1) ...
Authoritative Answer
Query for Amazon.com type=255 class=1
amazon.com HINFO (Host Info) Cpu:RFC8482 Os:
amazon.com NS (Nameserver) pdns1.ultradns.net
amazon.com NS (Nameserver) ns4.p31.dynect.net
amazon.com NS (Nameserver) ns3.p31.dynect.net
amazon.com NS (Nameserver) ns2.p31.dynect.net
```

```
amazon.com NS (Nameserver) ns2.p31.dynect.net
amazon.com NS (Nameserver) ns1.p31.dynect.net
amazon.com NS (Nameserver) pdns6.ultradns.co.uk
Dig Amazon.com@ns1.p31.dynect.net (208.78.70.31) ...
Authoritative Answer
Query for Amazon.com type=255 class=1
amazon.com SOA (Zone of Authority)
    Primary NS: dns-external-master.Amazon.com
    Responsible person: root@Amazon.com
    serial:2010131665
    refresh:180s (3 minutes)
    retry:60s
    expire:3024000s (35 days)
    minimum-ttl:60s
Amazon.com NS (Nameserver) ns3.p31.dynect.net
Amazon.com NS (Nameserver) ns2.p31.dynect.net
Amazon.com NS (Nameserver) ns1.p31.dynect.net
Amazon.com NS (Nameserver) pdns6.ultradns.co.uk
Amazon.com NS (Nameserver) pdns1.ultradns.net
Amazon.com NS (Nameserver) ns4.p31.dynect.net
Amazon.com A (Address) 176.32.103.205
Amazon.com A (Address) 54.239.28.85
```

```
Amazon.com A (Address) 54.239.28.85
Amazon.com A (Address) 205.251.242.103
Amazon.com MX (Mail Exchanger) Priority: 5 amazon-smtp.Amazon.com
Amazon.com TXT (Text Field)
    v=spf1 include:spf1.amazon.com include:spf2.amazon.com include:amazonses.com -all
    □ wwHqOq0HKhb7rDQAD GMxM2MzNzJmNWJlY2U5ZDU4MmVlNzQ2NWU4MTY5OWJjMjlmYjQ4Mjc5M2JiMzky
    facebook-domain-verification=d9u57u52gylohx845ogolaxzpywpmq
    □ WJmOTEwMGMxM2MzNzJmNWJlY2U5ZDU4MmVlNzQ2NWU4MTY5OWJjMjlmYjQ4Mjc5M2JiMzkyAD Amazon
    MS=4B600B22799EB2CAC0D8FF0A3A3CAECA5EE2BF3A
    □ jQ4Mjc5M2JiMzkyAD Amazon.com TXT (Text Field)
    google-site-verification=14WGw2MdmNMxchG8PlinF7LgqqE0OwwHqOq0HKhb7rDQ
    □ Amazon.com TXT (Text Field)
    wrike-verification=MzI3NzM2ODo2NDk5MjE4NjQ2MmWJmOTEwMGMxM2MzNzJmNWJlY2U5ZDU4MmVlNzQ2NWU
    Amazon.com TXT (Text Field)
    spf2.0/pra include:spf1.amazon.com include:spf2.amazon.com include:amazonses.com -all
Dig Amazon.com@ns4.p31.dynect.net (204.13.251.31) ...
Authoritative Answer
Query for Amazon.com type=255 class=1
amazon.com SOA (Zone of Authority)
    Primary NS: dns-external-master.Amazon.com
    Responsible person: root@Amazon.com
    serial:2010131665
```



```

serial:2010131665
refresh:180s (3 minutes)
retry:60s
expire:3024000s (35 days)
minimum-ttl:60s
Amazon.com NS (Nameserver) ns2.p31.dynect.net
Amazon.com NS (Nameserver) ns1.p31.dynect.net
Amazon.com NS (Nameserver) pdns6.ultradns.co.uk
Amazon.com NS (Nameserver) pdns1.ultradns.net
Amazon.com NS (Nameserver) ns3.p31.dynect.net
Amazon.com NS (Nameserver) ns4.p31.dynect.net
Amazon.com A (Address) 176.32.103.205
Amazon.com A (Address) 54.239.28.85
Amazon.com A (Address) 205.251.242.103
Amazon.com MX (Mail Exchanger) Priority: 5 amazon-smtp.Amazon.com
Amazon.com TXT (Text Field)
    spf2.0/prä include:spf1.amazon.com include:spf2.amazon.com include:amazonses.com -all
    □ MdNMxchg8PlinF7LgqqE0OwwHqOq0HKhb7rDQÄÄ acebook-domain-verification=d9u57u52gylohx845ogolaxzpywpmq
Amazon.com TXT (Text Field)
    v=spf1 include:spf1.amazon.com include:spf2.amazon.com include:amazonses.com -all
    □ 45ogolaxzpywpmqÄÄ o2NDk5Mje4NjQ2MWJmOTeWmGMxM2MzNzJmNWJlY2U5ZDU4MmVlNzQ2NWU4MjY5OWJjMjlmYjQ4Mjc5
Amazon.com TXT (Text Field)
    v=spf1 include:spf1.amazon.com include:spf2.amazon.com include:amazonses.com -all
    □ 45ogolaxzpywpmqÄÄ o2NDk5Mje4NjQ2MWJmOTeWmGMxM2MzNzJmNWJlY2U5ZDU4MmVlNzQ2NWU4MjY5OWJjMjlmYjQ4Mjc5
Amazon.com TXT (Text Field)
    v=spf1 include:spf1.amazon.com include:spf2.amazon.com include:amazonses.com -all
    □ 45ogolaxzpywpmqÄÄ o2NDk5Mje4NjQ2MWJmOTeWmGMxM2MzNzJmNWJlY2U5ZDU4MmVlNzQ2NWU4MjY5OWJjMjlmYjQ4Mjc5
Amazon.com TXT (Text Field)
    MS=4B600B22799EB2CAC0D8FF0A3A3CAECA5EE2BF3A
    □ Do2NDk5Mje4NjQ2MWJmOTeWmGMxM2MzNzJmNWJlY2U5ZDU4MmVlNzQ2NWU4MTY5OWJjMjlmYjQ4Mjc5
Amazon.com TXT (Text Field)
    google-site-verification=14WGW2MdNMxchg8PlinF7LgqqE0OwwHqOq0HKhb7rDQ
    □ Amazon.com TXT (Text Field)
    facebook-domain-verification=d9u57u52gylohx845ogolaxzpywpmq
Amazon.com TXT (Text Field)
    wrike-verification=MzI3NzM2ODo2NDk5Mje4NjQ2MWJmOTeWmGMxM2MzNzJmNWJlY2U5ZDU4MmVlNzQ2NWU4MjY5OWJjMjlmYjQ4Mjc5
Dig Amazon.com@172.30.0.11 ...
Non-authoritative answer
Recursive queries supported by this server
Query for Amazon.com type=255 class=1
Amazon.com TXT (Text Field)
    MS=4B600B22799EB2CAC0D8FF0A3A3CAECA5EE2BF3A
    □ om include:spf2.amazon.com include:amazonses.com -allÄÄ include:spf2.amazon.com include:amazonses.com -allÄÄ
    facebook-domain-verification=d9u57u52gylohx845ogolaxzpywpmq
    □ /pra include:spf1.amazon.com include:spf2.amazon.com include:amazonses.com -allÄÄ e-verification=MzI3NzM2ODo2NDk5Mje4NjQ2MWJmOTeWmGMxM2MzNzJmNWJlY2U5ZDU4MmVlNzQ2NWU4MjY5OWJjMjlmYjQ4Mjc5
com include:amazonses.com -allÄÄ e-verification=MzI3NzM2ODo2NDk5Mje4NjQ2MWJmOTeWmGMxM2MzNzJmNWJlY2U5ZDU4MmVlNzQ2NWU4MjY5OWJjMjlmYjQ4Mjc5
zkyÄÄ UÄÄ co
uk
Amazon.com TXT (Text Field)
    google-site-verification=14WGW2MdNMxchg8PlinF7LgqqE0OwwHqOq0HKhb7rDQ
    □ Amazon.com TXT (Text Field)
    v=spf1 include:spf1.amazon.com include:spf2.amazon.com include:amazonses.com -all
    □ NWU4MTY5OWJjMjlmYjQ4Mjc5M2JiMzkyÄÄ on-smtpÄÄÄÄ Amazon.com TXT (Text Field)
    spf2.0/prä include:spf1.amazon.com include:spf2.amazon.com include:amazonses.com -all
    □ Amazon.com TXT (Text Field)
    wrike-verification=MzI3NzM2ODo2NDk5Mje4NjQ2MWJmOTeWmGMxM2MzNzJmNWJlY2U5ZDU4MmVlNzQ2NWU4MjY5OWJjMjlmYjQ4Mjc5
    □ s1p1ultradnsÄÄÄÄ Amazon.com MX (Mail Exchanger) Priority: 5 amazon-smtp.Amazon.com
Amazon.com A (Address) 176.32.103.205
Amazon.com A (Address) 205.251.242.103
Amazon.com A (Address) 54.239.28.85
Amazon.com NS (Nameserver) pdns6.ultradns.co.uk
Amazon.com NS (Nameserver) ns1.p31.dynect.net
Amazon.com NS (Nameserver) ns3.p31.dynect.net
Amazon.com NS (Nameserver) ns4.p31.dynect.net
Amazon.com NS (Nameserver) pdns1.ultradns.net
Amazon.com NS (Nameserver) ns2.p31.dynect.net
Amazon.com SOA (Zone of Authority)

```

```
Amazon.com SOA (Zone of Authority)
  Primary NS: dns-external-master.Amazon.com
  Responsible person: root@Amazon.com
  serial:2010131665
  refresh:180s (3 minutes)
  retry:60s
  expire:3024000s (35 days)
  minimum-ttl:60s
Amazon.com NS (Nameserver) pdns1.ultradns.net
Amazon.com NS (Nameserver) ns1.p31.dynect.net
Amazon.com NS (Nameserver) pdns6.ultradns.co.uk
Amazon.com NS (Nameserver) ns2.p31.dynect.net
Amazon.com NS (Nameserver) ns3.p31.dynect.net
Amazon.com NS (Nameserver) ns4.p31.dynect.net
```

## Nslookup Command Prompt for Amazon.com

```
C:\Users\Administrator>nslookup
Default Server: dns.google
Address: 8.8.8.8

> set type=any
> Amazon.com
Server: dns.google
Address: 8.8.8.8

Non-authoritative answer:
Amazon.com
  primary name server = dns-external-master.Amazon.com
  responsible mail addr = root.Amazon.com
  serial = 2010131667
  refresh = 180 (3 mins)
  retry = 60 (1 min)
  expire = 3024000 (35 days)
  default TTL = 60 (1 min)
Amazon.com nameserver = ns4.p31.dynect.net
Amazon.com nameserver = ns2.p31.dynect.net
Amazon.com nameserver = ns1.p31.dynect.net
Amazon.com nameserver = ns3.p31.dynect.net
Amazon.com nameserver = pdns6.ultradns.co.uk
Amazon.com nameserver = pdns1.ultradns.net
Amazon.com internet address = 205.251.242.103
Amazon.com internet address = 54.239.28.85
Amazon.com internet address = 176.32.103.205
Amazon.com MX preference = 5, mail exchanger = amazon-smtp.Amazon.com
Amazon.com text =

"unlike-verification=MzT3NzQ2ODQ2NDk5MDE4NjQ2MmU7m0TEwMGMxM2MzNzTmNlWjV2UjU5ZDU4MmVlNzQ2MmU4MTY5QWVlM41mV4Q4MDErSM
```

```

"write-verification=MzI3NzM2ODo2NDk5MjE4NjQ2MWJmOTewMGxM2MzNzJmNWJlY2U5ZDU4MmVlNzQ2NWU4MTY5OWJjMjlmYjQ4Mjc5M
23iMzky"
Amazon.com      text =

"MS=4B600B22799EB2CAC0D8FF0A3A3CAECA5EE2BF3A"
Amazon.com      text =

"v=spf1 include:spf1.amazon.com include:spf2.amazon.com include:amazonses.com -all"
Amazon.com      text =

"facebook-domain-verification=d9u57u52gylohx845ogoiaxzpywpmq"
Amazon.com      text =

"google-site-verification=14WGW2MdNMxchG8PlinF7LgqqE00wwHqOq0HKhb7rDQ"
Amazon.com      text =

"spf2.0/pra include:spf1.amazon.com include:spf2.amazon.com include:amazonses.com -all"
> _

```

## Amazon IP Address

```

> 205.251.242.103
Server:  dns.google
Address:  8.8.8.8

Name:     s3-console-us-standard.console.aws.amazon.com
Address:  205.251.242.103

```

## Service Oriented Architecture (SOA) Command Prompt Amazon.com

```

> set type=soa
> Amazon.com
Server:  dns.google
Address:  8.8.8.8

Non-authoritative answer:
Amazon.com
      primary name server = dns-external-master.Amazon.com
      responsible mail addr = root.Amazon.com
      serial      = 2010131667
      refresh    = 180 (3 mins)
      retry      = 60 (1 min)
      expire     = 3024000 (35 days)
      default TTL = 60 (1 min)
> _

```

## Cloudparadox.com Source Code Secret Message

```
        </div>
<!-- Secret message: congratulations you have found the secret message. Take a screen shot of this message
    </div>
    </div>
    </div>
</body>
</html>
```

CE PROSPECTION | Powered By: Security Centric Inc &reg;</p>

have found the secret message. Take a screen shot of this message and add it to your lab work file. -->

## Cloudparadox.com Sam Spade Source Code Secret Message

```
        </div>
<!-- Secret message: congratulations you have found the secret message. Take a screen shot of this message
    </div>
    </div>
    </div>
</body>
```

message. Take a screen shot of this message and add it to your lab work file. -->