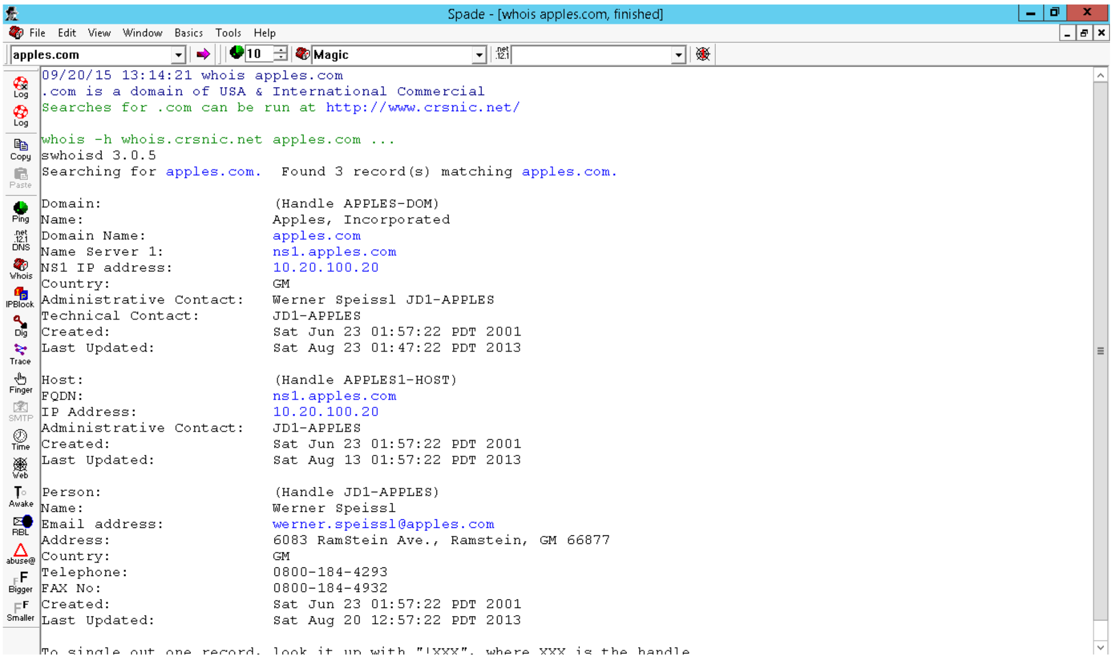
Lab Report

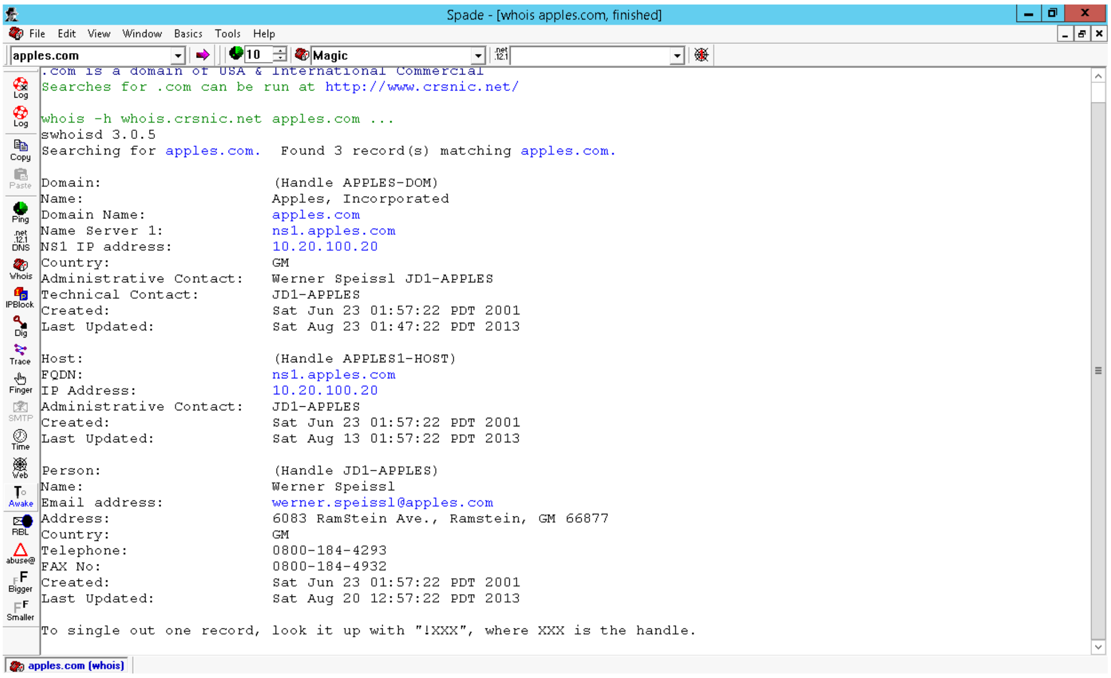
1. Whois report results for three domains

1.1 Apples.com

1.1.1 Whois result screenshot



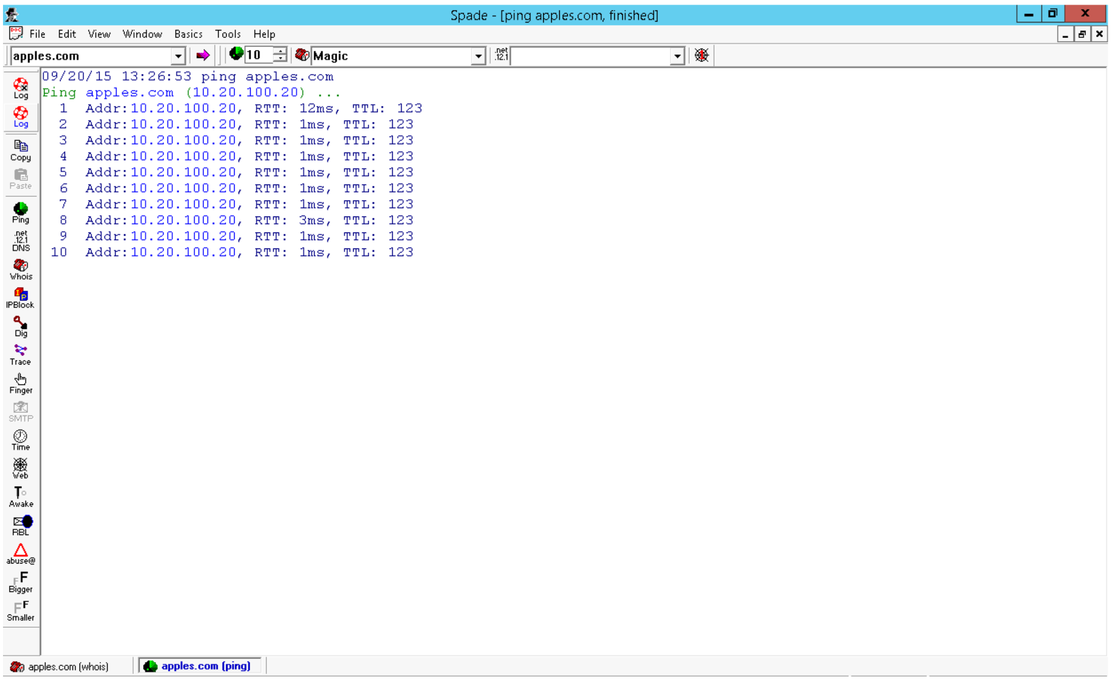
```
09/20/15 13:14:21 whois apples.com
.com is a domain of USA & International Commercial
Searches for .com can be run at http://www.crsnic.net/

whois -h whois.crsnic.net apples.com ...
swhoisd 3.0.5
Searching for apples.com.  Found 3 record(s) matching apples.com.

Domain:                   (Handle APPLES-DOM)
Name:                     Apples, Incorporated
Domain Name:              apples.com
Name Server 1:            ns1.apples.com
NS1 IP address:           10.20.100.20
Country:                  GM
Administrative Contact:   Werner Speissl JD1-APPLES
Technical Contact:        JD1-APPLES
Created:                  Sat Jun 23 01:57:22 PDT 2001
Last Updated:             Sat Aug 23 01:47:22 PDT 2013

Host:                     (Handle APPLES1-HOST)
FQDN:                     ns1.apples.com
IP Address:               10.20.100.20
Administrative Contact:   JD1-APPLES
Created:                  Sat Jun 23 01:57:22 PDT 2001
Last Updated:             Sat Aug 13 01:57:22 PDT 2013

Person:                   (Handle JD1-APPLES)
Name:                     Werner Speissl
Email address:            werner.speissl@apples.com
Address:                  6083 RamStein Ave., Ramstein, GM 66877
Country:                  GM
Telephone:                0800-184-4293
FAX No:                   0800-184-4932
Created:                  Sat Jun 23 01:57:22 PDT 2001
Last Updated:             Sat Aug 20 12:57:22 PDT 2013

To single out one record, look it up with "!XXX", where XXX is the handle
```



```
.com is a domain of USA & International Commercial
Searches for .com can be run at http://www.crsnic.net/

whois -h whois.crsnic.net apples.com ...
swhoisd 3.0.5
Searching for apples.com.  Found 3 record(s) matching apples.com.

Domain:                   (Handle APPLES-DOM)
Name:                     Apples, Incorporated
Domain Name:              apples.com
Name Server 1:            ns1.apples.com
NS1 IP address:           10.20.100.20
Country:                  GM
Administrative Contact:   Werner Speissl JD1-APPLES
Technical Contact:        JD1-APPLES
Created:                  Sat Jun 23 01:57:22 PDT 2001
Last Updated:             Sat Aug 23 01:47:22 PDT 2013

Host:                     (Handle APPLES1-HOST)
FQDN:                     ns1.apples.com
IP Address:               10.20.100.20
Administrative Contact:   JD1-APPLES
Created:                  Sat Jun 23 01:57:22 PDT 2001
Last Updated:             Sat Aug 13 01:57:22 PDT 2013

Person:                   (Handle JD1-APPLES)
Name:                     Werner Speissl
Email address:            werner.speissl@apples.com
Address:                  6083 RamStein Ave., Ramstein, GM 66877
Country:                  GM
Telephone:                0800-184-4293
FAX No:                   0800-184-4932
Created:                  Sat Jun 23 01:57:22 PDT 2001
Last Updated:             Sat Aug 20 12:57:22 PDT 2013

To single out one record, look it up with "!XXX", where XXX is the handle.
```

Description: it shows all critical information like hostname, organization name, possible location, created time, update time, domain user information, administrator and technical contact.

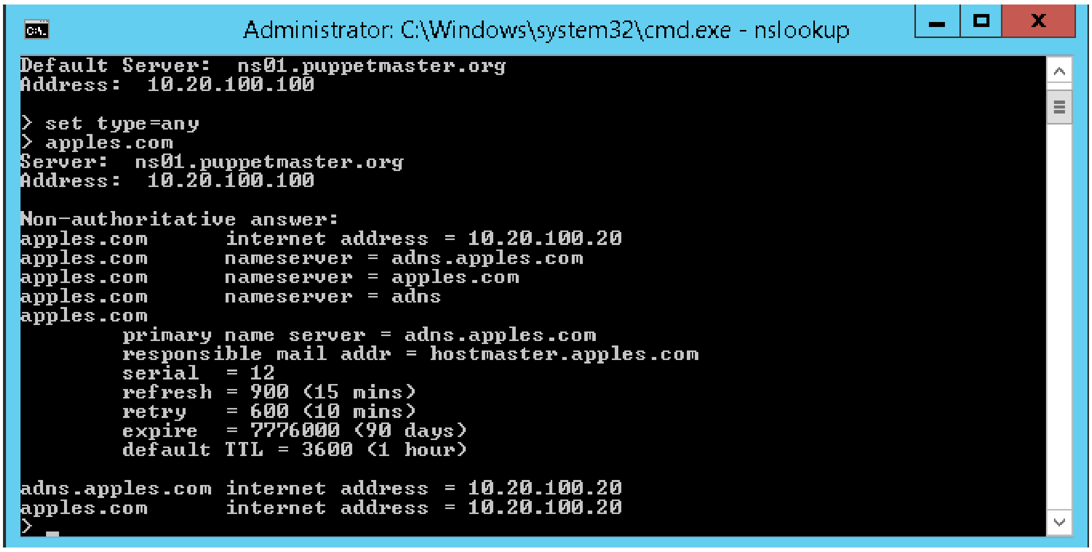
1.1.2 Ping result screenshot



```
09/20/15 13:26:53 ping apples.com
Ping apples.com (10.20.100.20) ...
  1   Addr:10.20.100.20, RTT: 12ms, TTL: 123
  2   Addr:10.20.100.20, RTT: 1ms, TTL: 123
  3   Addr:10.20.100.20, RTT: 1ms, TTL: 123
  4   Addr:10.20.100.20, RTT: 1ms, TTL: 123
  5   Addr:10.20.100.20, RTT: 1ms, TTL: 123
  6   Addr:10.20.100.20, RTT: 1ms, TTL: 123
  7   Addr:10.20.100.20, RTT: 1ms, TTL: 123
  8   Addr:10.20.100.20, RTT: 3ms, TTL: 123
  9   Addr:10.20.100.20, RTT: 1ms, TTL: 123
 10   Addr:10.20.100.20, RTT: 1ms, TTL: 123
```

Description: use ping command to check whether target is alive or not.

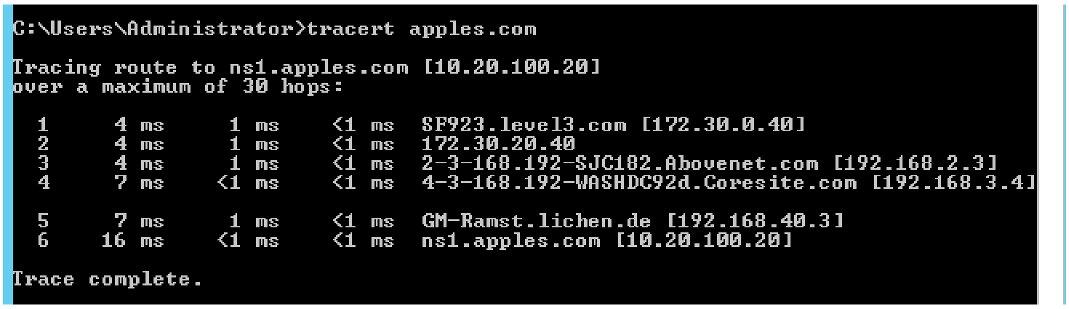
1.1.3 Nslookup result screenshot



```
Default Server:  ns01.puppetmaster.org
Address:  10.20.100.100

> set type=any
> apples.com
Server:  ns01.puppetmaster.org
Address:  10.20.100.100

Non-authoritative answer:
apples.com      internet address = 10.20.100.20
apples.com      nameserver = adns.apples.com
apples.com      nameserver = apples.com
apples.com      nameserver = adns
apples.com
        primary name server = adns.apples.com
        responsible mail addr = hostmaster.apples.com
        serial  = 12
        refresh = 900 (15 mins)
        retry   = 600 (10 mins)
        expire  = 7776000 (90 days)
        default TTL = 3600 (1 hour)

adns.apples.com internet address = 10.20.100.20
apples.com      internet address = 10.20.100.20
> _
```

Description: it shows information about DNS server.

1.1.4 Tracert results screenshot

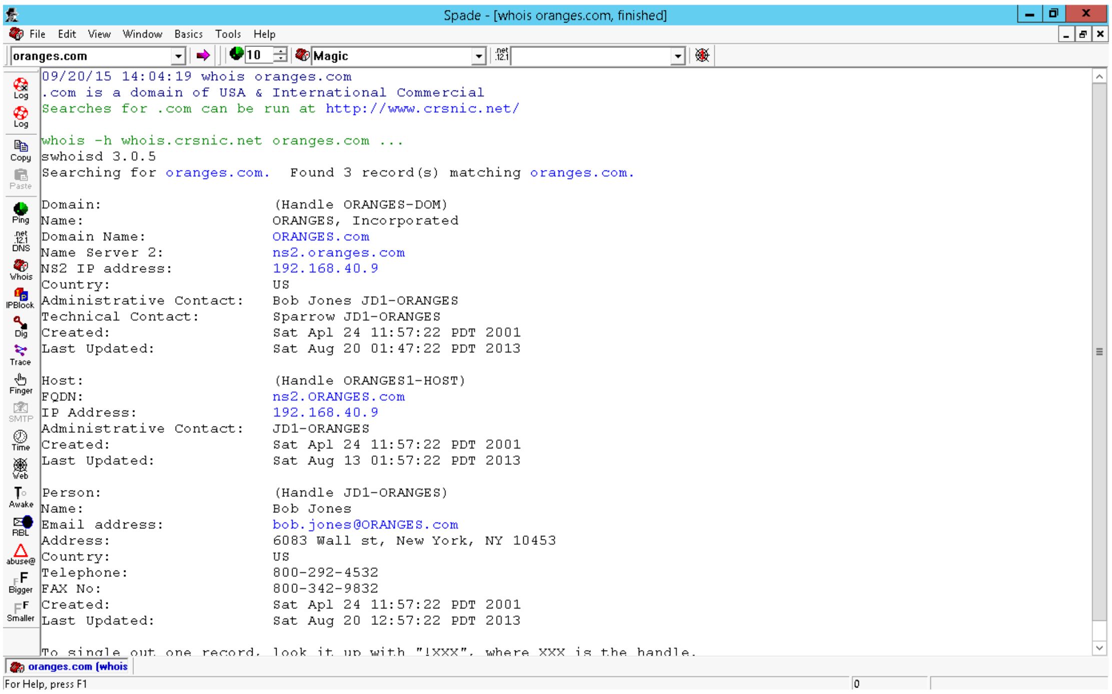


```
C:\Users\Administrator>tracert apples.com

Tracing route to ns1.apples.com [10.20.100.20]
over a maximum of 30 hops:

  1     4 ms     1 ms    <1 ms  SF923.level3.com [172.30.0.40]
  2     4 ms     1 ms    <1 ms  172.30.20.40
  3     4 ms     1 ms    <1 ms  2-3-168.192-SJC182.Abovenet.com [192.168.2.3]
  4     7 ms    <1 ms    <1 ms  4-3-168.192-WASHDC92d.Coresite.com [192.168.3.4]

  5     7 ms     1 ms    <1 ms  GM-Ramst.lichen.de [192.168.40.3]
  6    16 ms    <1 ms    <1 ms  ns1.apples.com [10.20.100.20]

Trace complete.
```

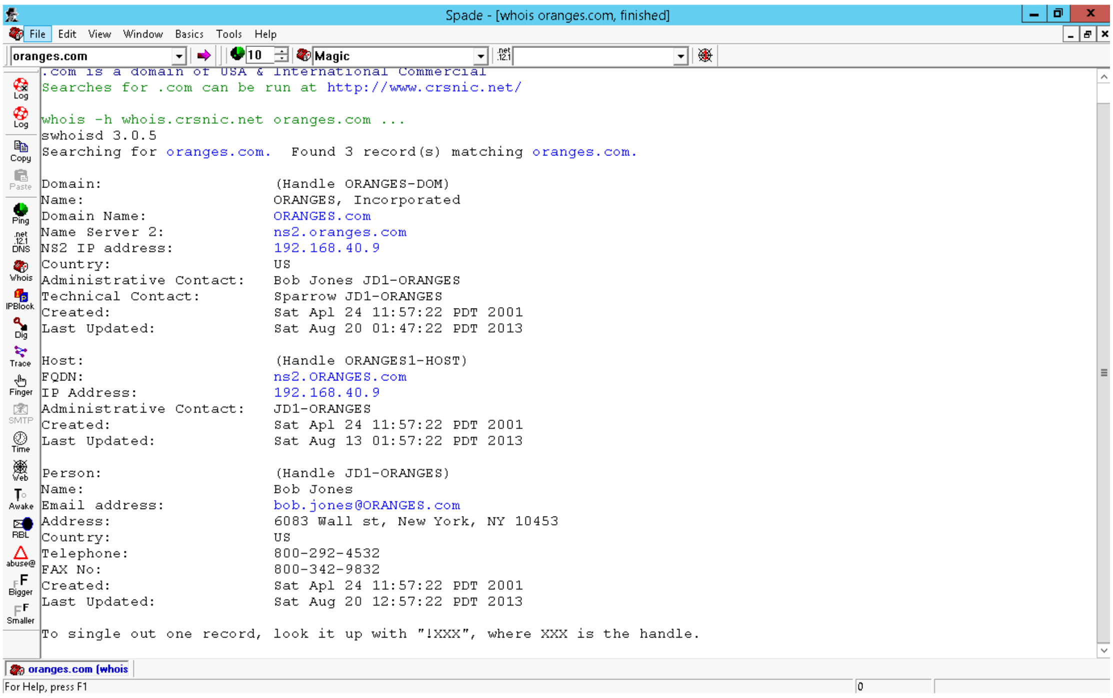
Description: it shows how many network nodes are there from Vworkstation desktop to apples.com and the detail things about each node.

1.2 Oranges.com

1.2.1 Whois result screenshot



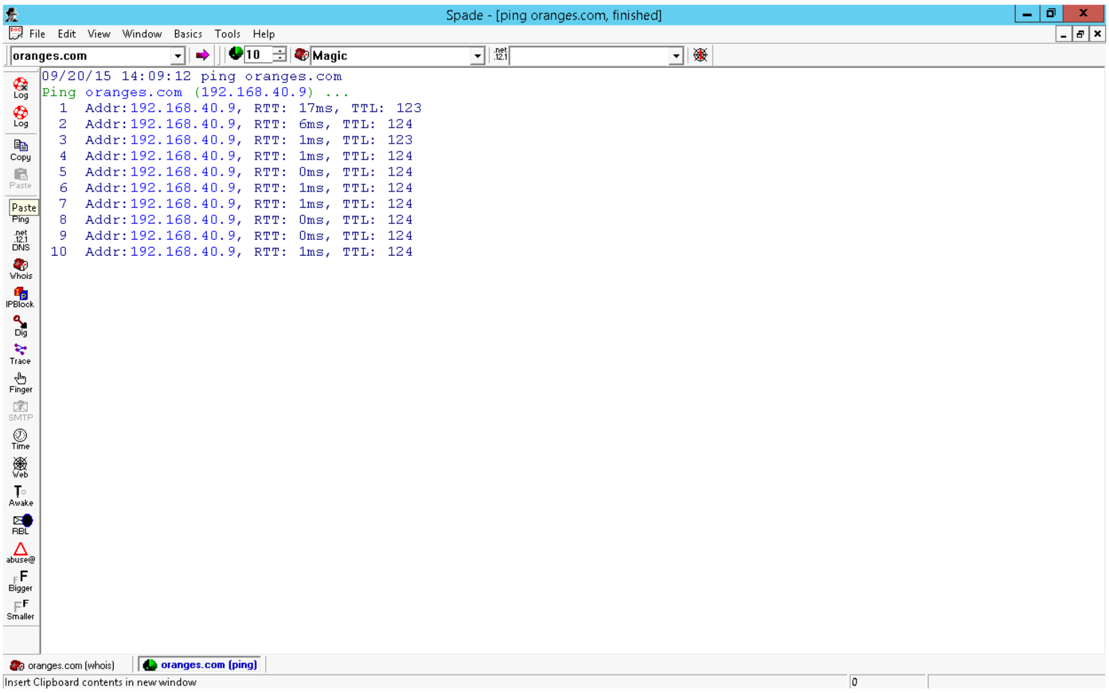
```
09/20/15 14:04:19 whois oranges.com
.com is a domain of USA & International Commercial
Searches for .com can be run at http://www.crsnic.net/

whois -h whois.crsnic.net oranges.com ...
swhoisd 3.0.5
Searching for oranges.com.  Found 3 record(s) matching oranges.com.

Domain:                     (Handle ORANGES-DOM)
Name:                       ORANGES, Incorporated
Domain Name:                ORANGES.com
Name Server 2:              ns2.oranges.com
NS2 IP address:             192.168.40.9
Country:                    US
Administrative Contact:     Bob Jones JD1-ORANGES
Technical Contact:          Sparrow JD1-ORANGES
Created:                    Sat Apl 24 11:57:22 PDT 2001
Last Updated:               Sat Aug 20 01:47:22 PDT 2013

Host:                       (Handle ORANGES1-HOST)
FQDN:                       ns2.ORANGES.com
IP Address:                 192.168.40.9
Administrative Contact:     JD1-ORANGES
Created:                    Sat Apl 24 11:57:22 PDT 2001
Last Updated:               Sat Aug 13 01:57:22 PDT 2013

Person:                     (Handle JD1-ORANGES)
Name:                       Bob Jones
Email address:              bob.jones@ORANGES.com
Address:                    6083 Wall st, New York, NY 10453
Country:                    US
Telephone:                  800-292-4532
FAX No:                     800-342-9832
Created:                    Sat Apl 24 11:57:22 PDT 2001
Last Updated:               Sat Aug 20 12:57:22 PDT 2013

To single out one record, look it up with "!XXX", where XXX is the handle.
```



```
.com is a domain of USA & International Commercial
Searches for .com can be run at http://www.crsnic.net/

whois -h whois.crsnic.net oranges.com ...
swhoisd 3.0.5
Searching for oranges.com.  Found 3 record(s) matching oranges.com.

Domain:                   (Handle ORANGES-DOM)
Name:                     ORANGES, Incorporated
Domain Name:              ORANGES.com
Name Server 2:            ns2.oranges.com
NS2 IP address:           192.168.40.9
Country:                  US
Administrative Contact:   Bob Jones JD1-ORANGES
Technical Contact:        Sparrow JD1-ORANGES
Created:                  Sat Apl 24 11:57:22 PDT 2001
Last Updated:             Sat Aug 20 01:47:22 PDT 2013

Host:                     (Handle ORANGES1-HOST)
FQDN:                     ns2.ORANGES.com
IP Address:               192.168.40.9
Administrative Contact:   JD1-ORANGES
Created:                  Sat Apl 24 11:57:22 PDT 2001
Last Updated:             Sat Aug 13 01:57:22 PDT 2013

Person:                   (Handle JD1-ORANGES)
Name:                     Bob Jones
Email address:            bob.jones@ORANGES.com
Address:                  6083 Wall st, New York, NY 10453
Country:                  US
Telephone:                800-292-4532
FAX No:                   800-342-9832
Created:                  Sat Apl 24 11:57:22 PDT 2001
Last Updated:             Sat Aug 20 12:57:22 PDT 2013

To single out one record, look it up with "!XXX", where XXX is the handle.
```

Description: it shows all critical information like hostname, organization name, possible location, created time, update time, domain user information, administrator and technical contact.

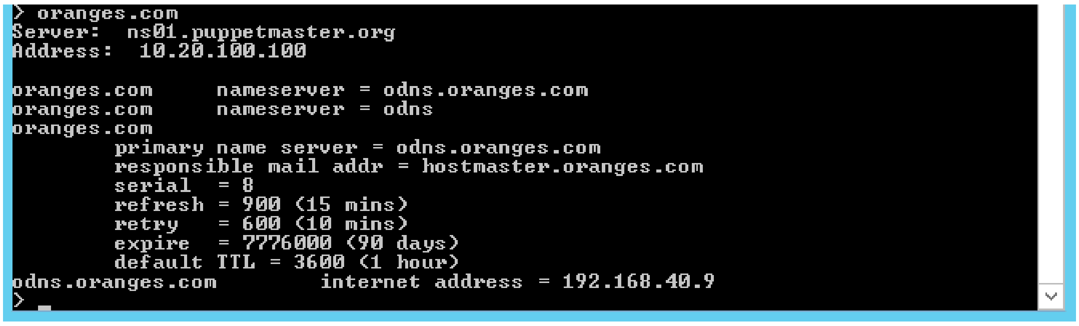
1.2.2 Ping result screenshot



```
09/20/15 14:09:12 ping oranges.com
Ping oranges.com (192.168.40.9) ...
  1  Addr:192.168.40.9, RTT: 17ms, TTL: 123
  2  Addr:192.168.40.9, RTT: 6ms, TTL: 124
  3  Addr:192.168.40.9, RTT: 1ms, TTL: 123
  4  Addr:192.168.40.9, RTT: 1ms, TTL: 124
  5  Addr:192.168.40.9, RTT: 0ms, TTL: 124
  6  Addr:192.168.40.9, RTT: 1ms, TTL: 124
  7  Addr:192.168.40.9, RTT: 1ms, TTL: 124
  8  Addr:192.168.40.9, RTT: 0ms, TTL: 124
  9  Addr:192.168.40.9, RTT: 0ms, TTL: 124
 10  Addr:192.168.40.9, RTT: 1ms, TTL: 124
```

Description: use ping command to check whether target is alive or not.

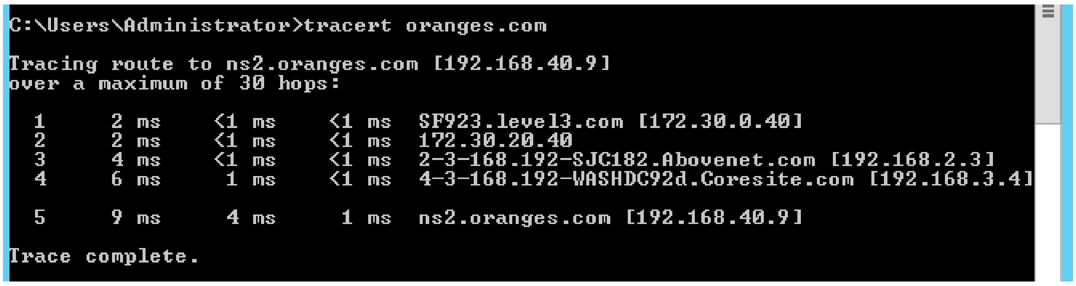
1.2.3 Nslookup result screenshot



```
> oranges.com
Server:  ns01.puppetmaster.org
Address:  10.20.100.100

oranges.com     nameserver = odns.oranges.com
oranges.com     nameserver = odns
oranges.com
        primary name server = odns.oranges.com
        responsible mail addr = hostmaster.oranges.com
        serial  = 8
        refresh = 900 (15 mins)
        retry   = 600 (10 mins)
        expire  = 7776000 (90 days)
        default TTL = 3600 (1 hour)
odns.oranges.com        internet address = 192.168.40.9
> _
```

Description: it shows information about DNS server.

1.2.4 Tracert results screenshot

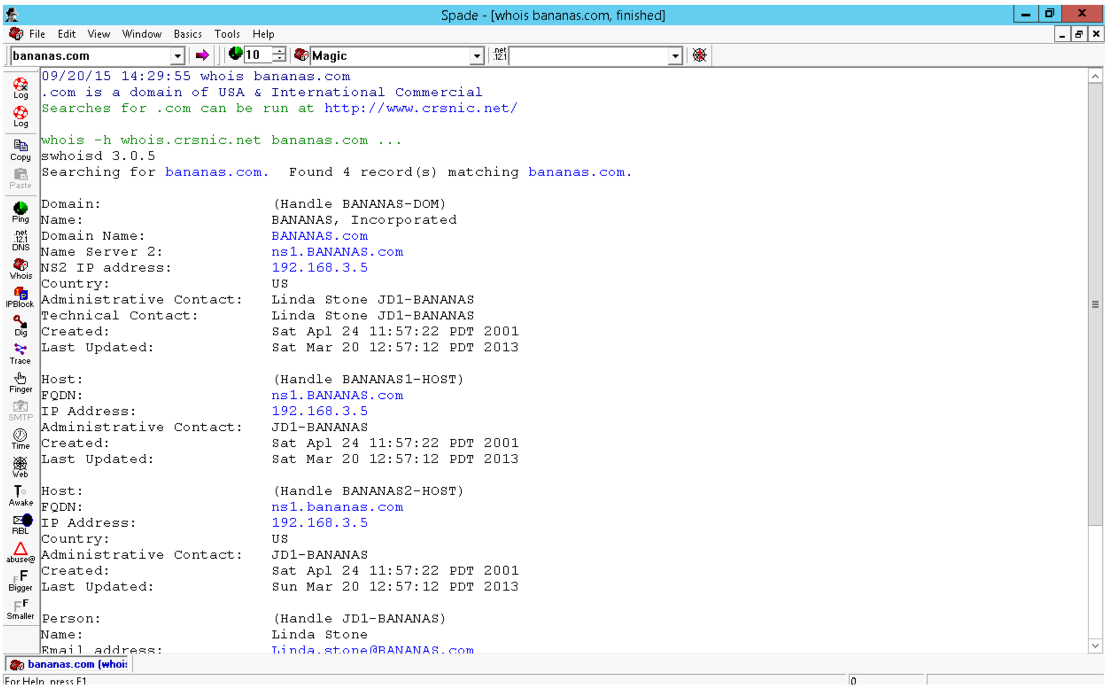


```
C:\Users\Administrator>tracert oranges.com

Tracing route to ns2.oranges.com [192.168.40.9]
over a maximum of 30 hops:

  1     2 ms    <1 ms    <1 ms  SF923.level3.com [172.30.0.40]
  2     2 ms    <1 ms    <1 ms  172.30.20.40
  3     4 ms    <1 ms    <1 ms  2-3-168.192-SJC182.Abovenet.com [192.168.2.3]
  4     6 ms     1 ms    <1 ms  4-3-168.192-WASHDC92d.Coresite.com [192.168.3.4]

  5     9 ms     4 ms     1 ms  ns2.oranges.com [192.168.40.9]

Trace complete.
```

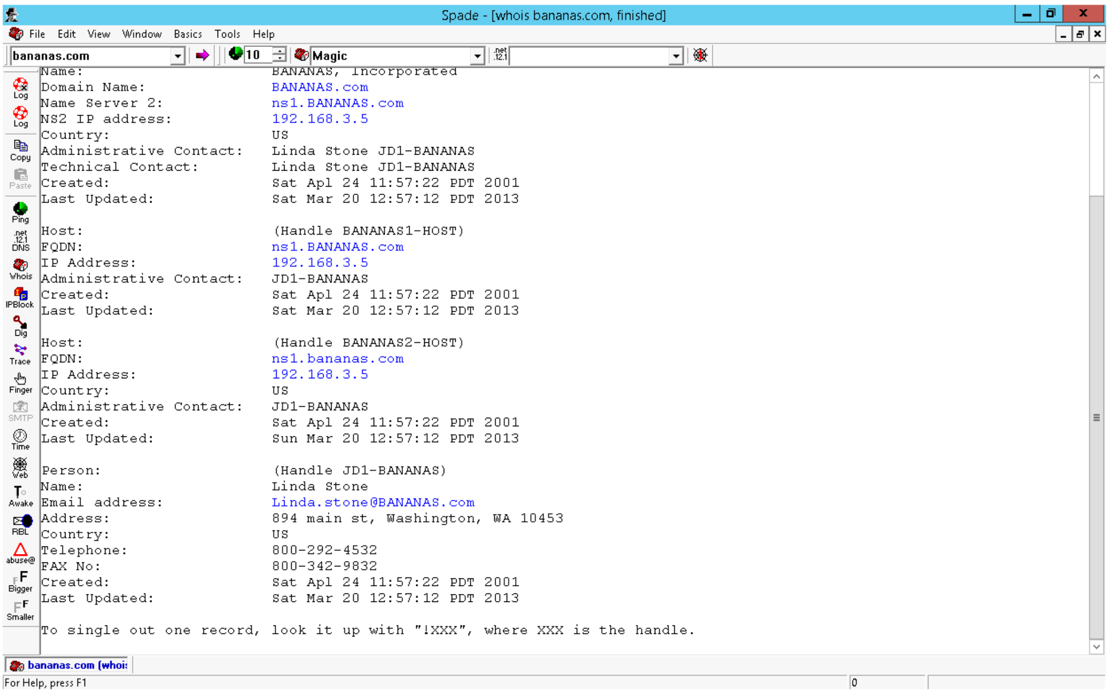
Description: it shows how many network nodes are there from Vworkstation desktop to apples.com and the detail things about each node.

1.3 Bananas.com

1.3.1 Whois results screenshot



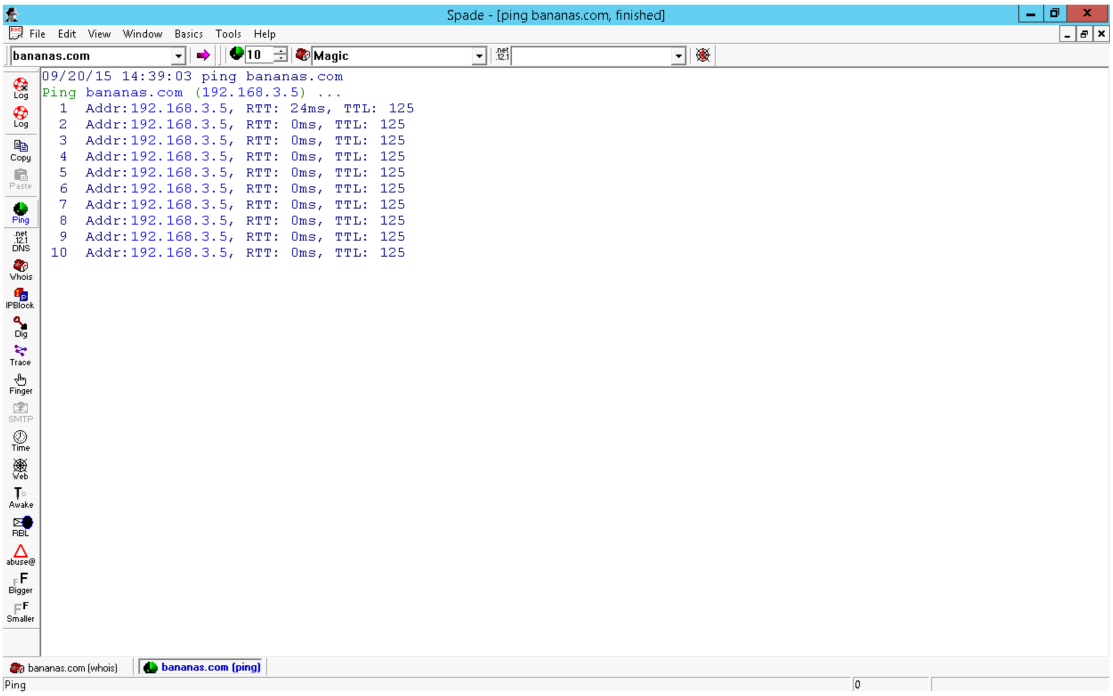
```
09/20/15 14:29:55 whois bananas.com
.com is a domain of USA & International Commercial
Searches for .com can be run at http://www.crsnic.net/

whois -h whois.crsnic.net bananas.com ...
swhoisd 3.0.5
Searching for bananas.com.  Found 4 record(s) matching bananas.com.

Domain:                    (Handle BANANAS-DOM)
Name:                      BANANAS, Incorporated
Domain Name:               BANANAS.com
Name Server 2:             ns1.BANANAS.com
NS2 IP address:            192.168.3.5
Country:                   US
Administrative Contact:    Linda Stone JD1-BANANAS
Technical Contact:         Linda Stone JD1-BANANAS
Created:                   Sat Apl 24 11:57:22 PDT 2001
Last Updated:              Sat Mar 20 12:57:12 PDT 2013

Host:                      (Handle BANANAS1-HOST)
FQDN:                      ns1.BANANAS.com
IP Address:                192.168.3.5
Administrative Contact:    JD1-BANANAS
Created:                   Sat Apl 24 11:57:22 PDT 2001
Last Updated:              Sat Mar 20 12:57:12 PDT 2013

Host:                      (Handle BANANAS2-HOST)
FQDN:                      ns1.bananas.com
IP Address:                192.168.3.5
Country:                   US
Administrative Contact:    JD1-BANANAS
Created:                   Sat Apl 24 11:57:22 PDT 2001
Last Updated:              Sun Mar 20 12:57:12 PDT 2013

Person:                    (Handle JD1-BANANAS)
Name:                      Linda Stone
Email address:             Linda.stone@BANANAS.com
```



```
Name:                     BANANAS, Incorporated
Domain Name:              BANANAS.com
Name Server 2:            ns1.BANANAS.com
NS2 IP address:           192.168.3.5
Country:                  US
Administrative Contact:   Linda Stone JD1-BANANAS
Technical Contact:        Linda Stone JD1-BANANAS
Created:                  Sat Apl 24 11:57:22 PDT 2001
Last Updated:             Sat Mar 20 12:57:12 PDT 2013

Host:                     (Handle BANANAS1-HOST)
FQDN:                     ns1.BANANAS.com
IP Address:               192.168.3.5
Administrative Contact:   JD1-BANANAS
Created:                  Sat Apl 24 11:57:22 PDT 2001
Last Updated:             Sat Mar 20 12:57:12 PDT 2013

Host:                     (Handle BANANAS2-HOST)
FQDN:                     ns1.bananas.com
IP Address:               192.168.3.5
Country:                  US
Administrative Contact:   JD1-BANANAS
Created:                  Sat Apl 24 11:57:22 PDT 2001
Last Updated:             Sun Mar 20 12:57:12 PDT 2013

Person:                   (Handle JD1-BANANAS)
Name:                     Linda Stone
Email address:            Linda.stone@BANANAS.com
Address:                  894 main st, Washington, WA 10453
Country:                  US
Telephone:                800-292-4532
FAX No:                   800-342-9832
Created:                  Sat Apl 24 11:57:22 PDT 2001
Last Updated:             Sat Mar 20 12:57:12 PDT 2013

To single out one record, look it up with "!XXX", where XXX is the handle.
```

Description: it shows all critical information like hostname, organization name, possible location, created time, update time, domain user information, administrator and technical contact.

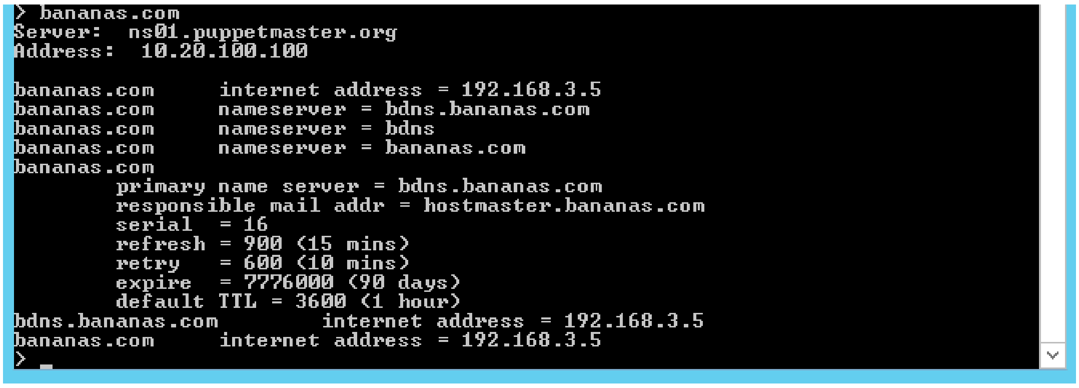
1.3.2 Ping results screenshot



```
09/20/15 14:39:03 ping bananas.com
Ping bananas.com (192.168.3.5) ...
  1  Addr:192.168.3.5, RTT: 24ms, TTL: 125
  2  Addr:192.168.3.5, RTT: 0ms, TTL: 125
  3  Addr:192.168.3.5, RTT: 0ms, TTL: 125
  4  Addr:192.168.3.5, RTT: 0ms, TTL: 125
  5  Addr:192.168.3.5, RTT: 0ms, TTL: 125
  6  Addr:192.168.3.5, RTT: 0ms, TTL: 125
  7  Addr:192.168.3.5, RTT: 0ms, TTL: 125
  8  Addr:192.168.3.5, RTT: 0ms, TTL: 125
  9  Addr:192.168.3.5, RTT: 0ms, TTL: 125
 10  Addr:192.168.3.5, RTT: 0ms, TTL: 125
```

Description: use ping command to check whether target is alive or not.

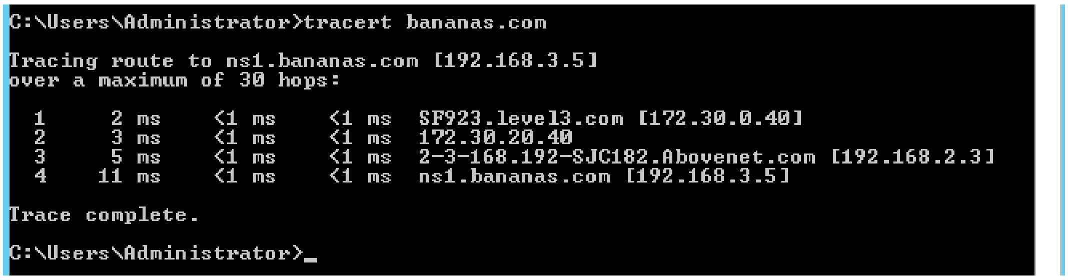
1.3.3 Nslookup results screenshot



```
> bananas.com
Server:  ns01.puppetmaster.org
Address:  10.20.100.100

bananas.com     internet address = 192.168.3.5
bananas.com     nameserver = bdns.bananas.com
bananas.com     nameserver = bdns
bananas.com     nameserver = bananas.com
bananas.com
        primary name server = bdns.bananas.com
        responsible mail addr = hostmaster.bananas.com
        serial  = 16
        refresh = 900 (15 mins)
        retry   = 600 (10 mins)
        expire  = 7776000 (90 days)
        default TTL = 3600 (1 hour)
bdns.bananas.com        internet address = 192.168.3.5
bananas.com     internet address = 192.168.3.5
> _
```

Description: it shows information about DNS server.

1.3.4 Tracert results screenshot



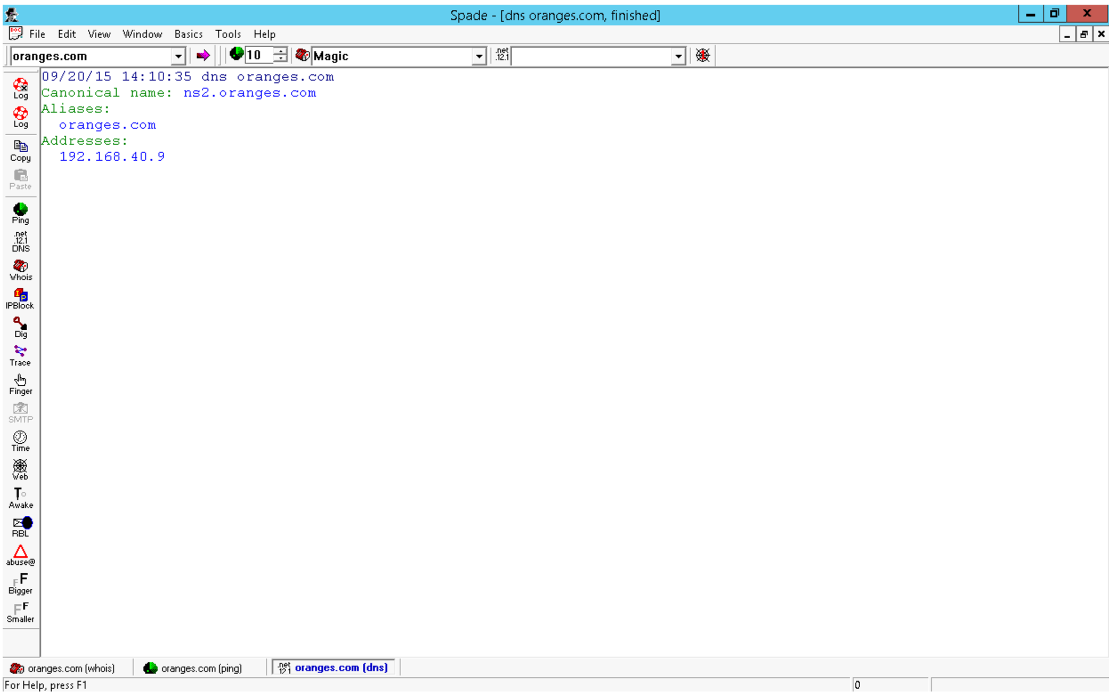
```
C:\Users\Administrator>tracert bananas.com

Tracing route to ns1.bananas.com [192.168.3.5]
over a maximum of 30 hops:

  1     2 ms    <1 ms    <1 ms  SF923.level3.com [172.30.0.40]
  2     3 ms    <1 ms    <1 ms  172.30.20.40
  3     5 ms    <1 ms    <1 ms  2-3-168.192-SJC182.Abovenet.com [192.168.2.3]
  4    11 ms    <1 ms    <1 ms  ns1.bananas.com [192.168.3.5]

Trace complete.

C:\Users\Administrator>_
```

Description: it shows how many network nodes are there from Vworkstation desktop to apples.com and the detail things about each node.

1.4 Tools in basic menu

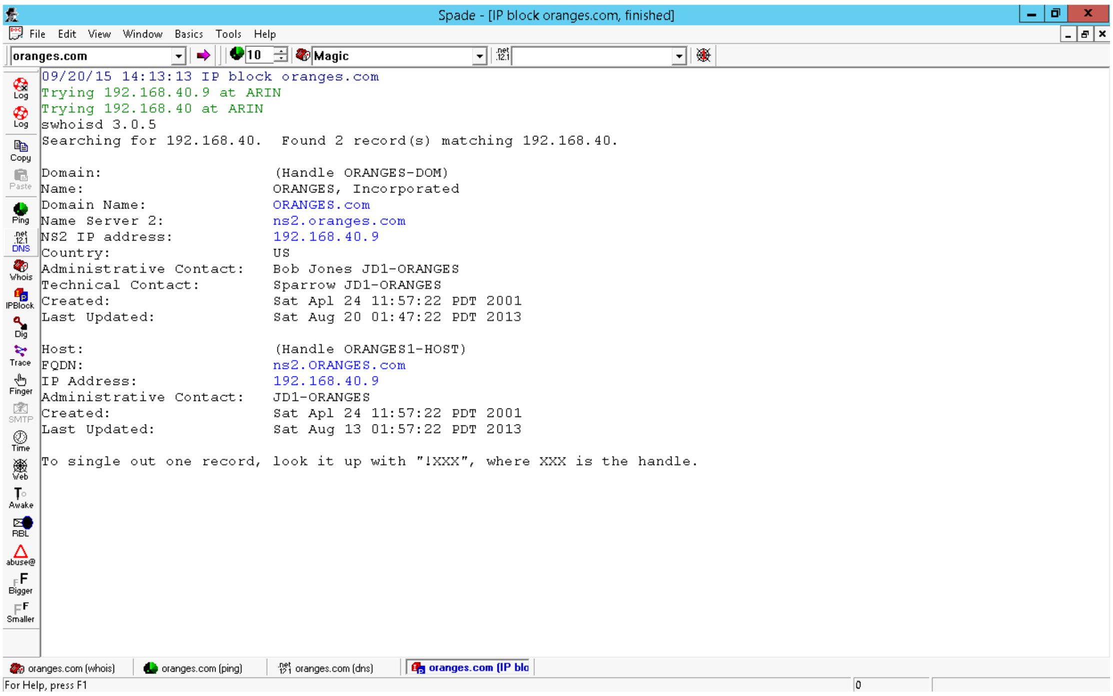
This part is used to descript each tool provided by Sam Spade in Basic menu, I just take Oranges.com as an example.

1.4.1 Nslookup



```
09/20/15 14:10:35 dns oranges.com
Canonical name: ns2.oranges.com
Aliases:
  oranges.com
Addresses:
  192.168.40.9
```

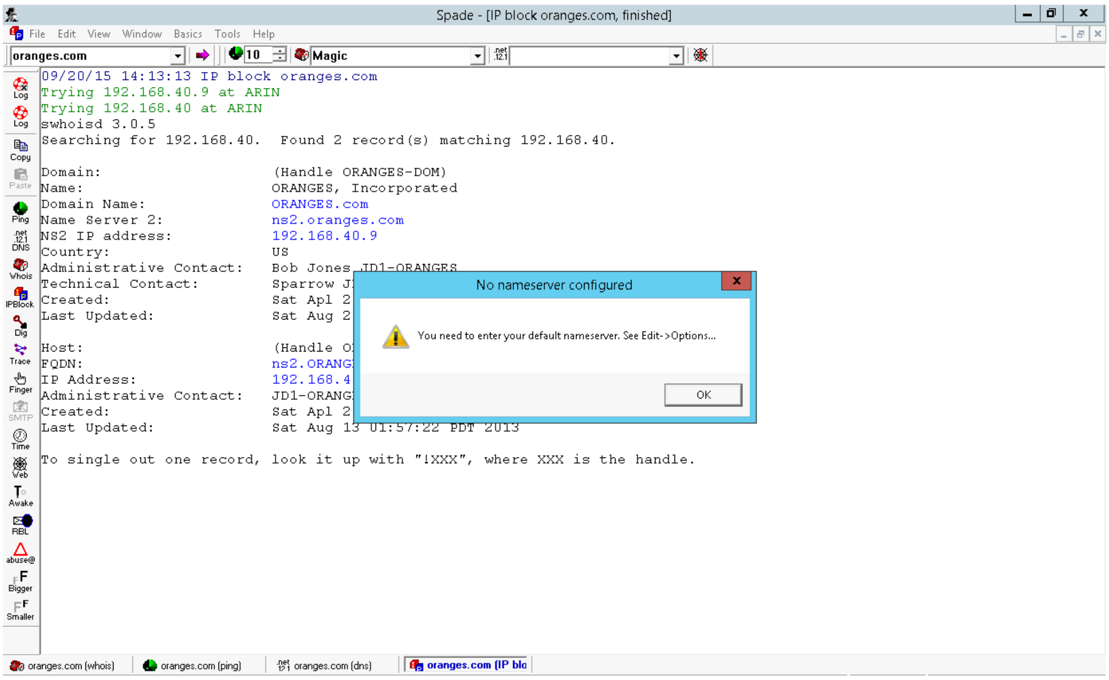
1.4.2 IP Block



```
09/20/15 14:13:13 IP block oranges.com
Trying 192.168.40.9 at ARIN
Trying 192.168.40 at ARIN
swhoisd 3.0.5
Searching for 192.168.40.  Found 2 record(s) matching 192.168.40.

Domain:                    (Handle ORANGES-DOM)
Name:                      ORANGES, Incorporated
Domain Name:               ORANGES.com
Name Server 2:             ns2.oranges.com
NS2 IP address:            192.168.40.9
Country:                   US
Administrative Contact:    Bob Jones JD1-ORANGES
Technical Contact:         Sparrow JD1-ORANGES
Created:                   Sat Apl 24 11:57:22 PDT 2001
Last Updated:              Sat Aug 20 01:47:22 PDT 2013

Host:                      (Handle ORANGES1-HOST)
FQDN:                      ns2.ORANGES.com
IP Address:                192.168.40.9
Administrative Contact:    JD1-ORANGES
Created:                   Sat Apl 24 11:57:22 PDT 2001
Last Updated:              Sat Aug 13 01:57:22 PDT 2013

To single out one record, look it up with "!XXX", where XXX is the handle.
```

Description: determine the ownership and contact information for a block of IP addresses. It is useful to determine specific information about a host and determine upstream Internet Service provider

1.4.3 Dig



```
09/20/15 14:13:13 IP block oranges.com
Trying 192.168.40.9 at ARIN
Trying 192.168.40 at ARIN
swhoisd 3.0.5
Searching for 192.168.40.  Found 2 record(s) matching 192.168.40.

Domain:                    (Handle ORANGES-DOM)
Name:                      ORANGES, Incorporated
Domain Name:               ORANGES.com
Name Server 2:             ns2.oranges.com
NS2 IP address:            192.168.40.9
Country:                   US
Administrative Contact:    Bob Jones JD1-ORANGES
Technical Contact:         Sparrow J
Created:                   Sat Apl 2
Last Updated:              Sat Aug 2

Host:                      (Handle O
FQDN:                      ns2.ORANG
IP Address:                192.168.4
Administrative Contact:    JD1-ORANG
Created:                   Sat Apl 2
Last Updated:              Sat Aug 13 01:57:22 PDT 2013

To single out one record, look it up with "!XXX", where XXX is the handle.
```

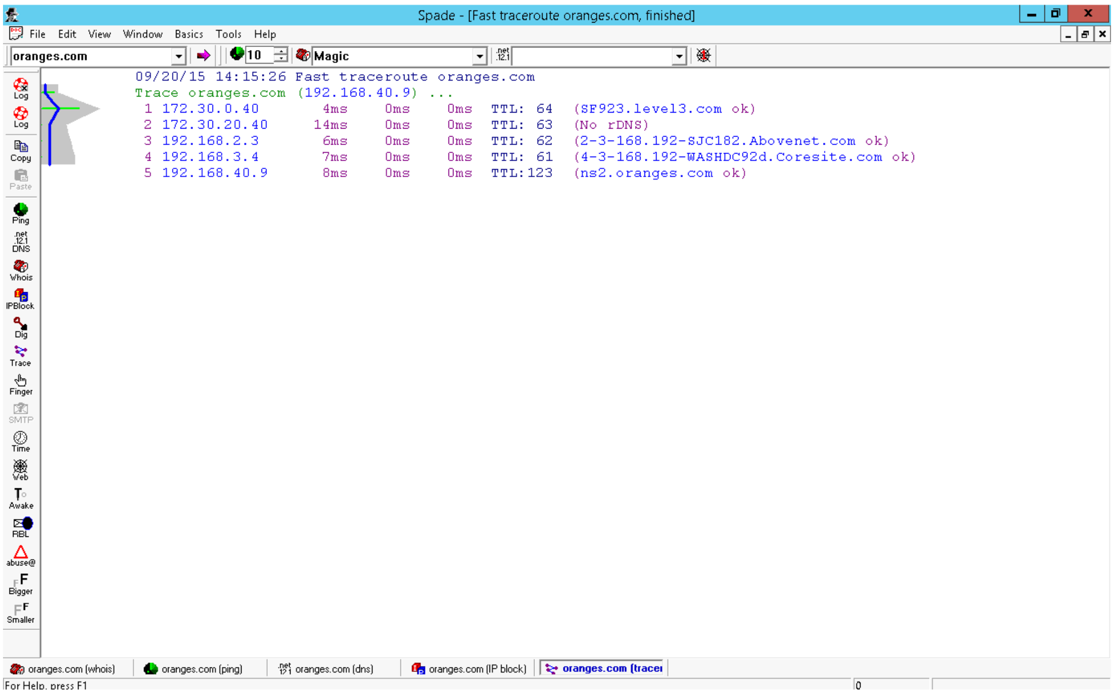
No nameserver configured

You need to enter your default nameserver. See Edit->Options...

OK

Description: an advanced DNS tool that returns all of the available Resource Records for a given domain or host.

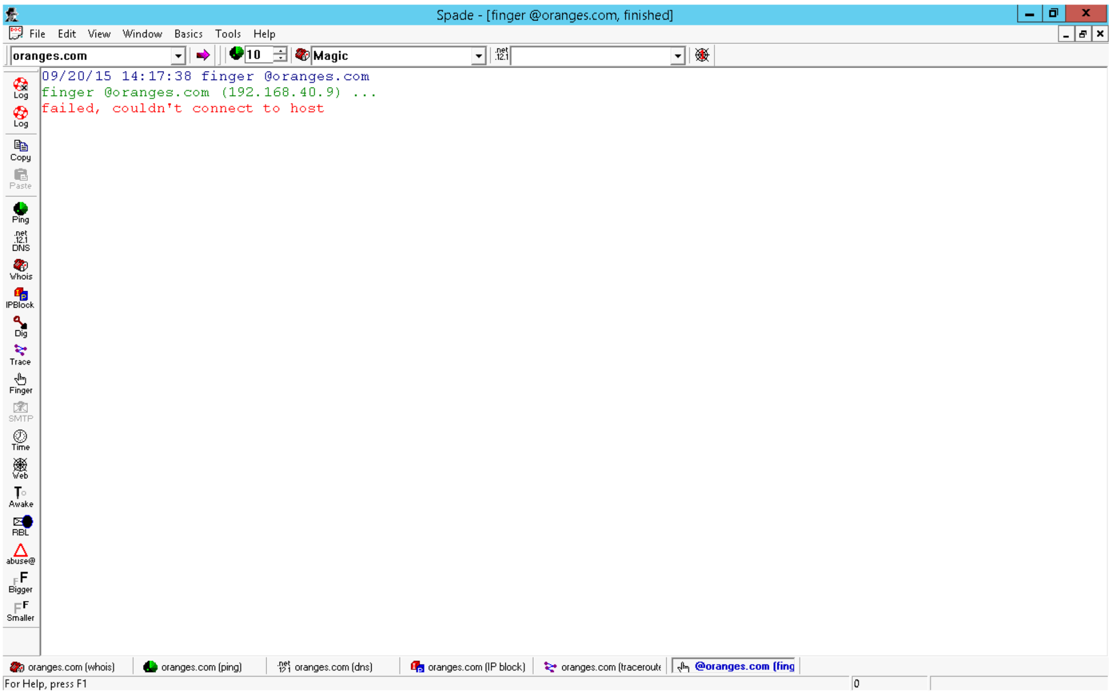
1.4.4 Traceroute



```
09/20/15 14:15:26 Fast traceroute oranges.com
Trace oranges.com (192.168.40.9) ...
 1 172.30.0.40      4ms    0ms    0ms  TTL: 64  (SF923.level3.com ok)
 2 172.30.20.40    14ms    0ms    0ms  TTL: 63  (No rDNS)
 3 192.168.2.3      6ms    0ms    0ms  TTL: 62  (2-3-168.192-SJC182.Abovenet.com ok)
 4 192.168.3.4      7ms    0ms    0ms  TTL: 61  (4-3-168.192-WASHDC92d.Coresite.com ok)
 5 192.168.40.9     8ms    0ms    0ms  TTL:123  (ns2.oranges.com ok)
```

Description: the route packets may take to the host specified in the address bar. Good for determining the upstream providers of internet service, and for identifying delays.

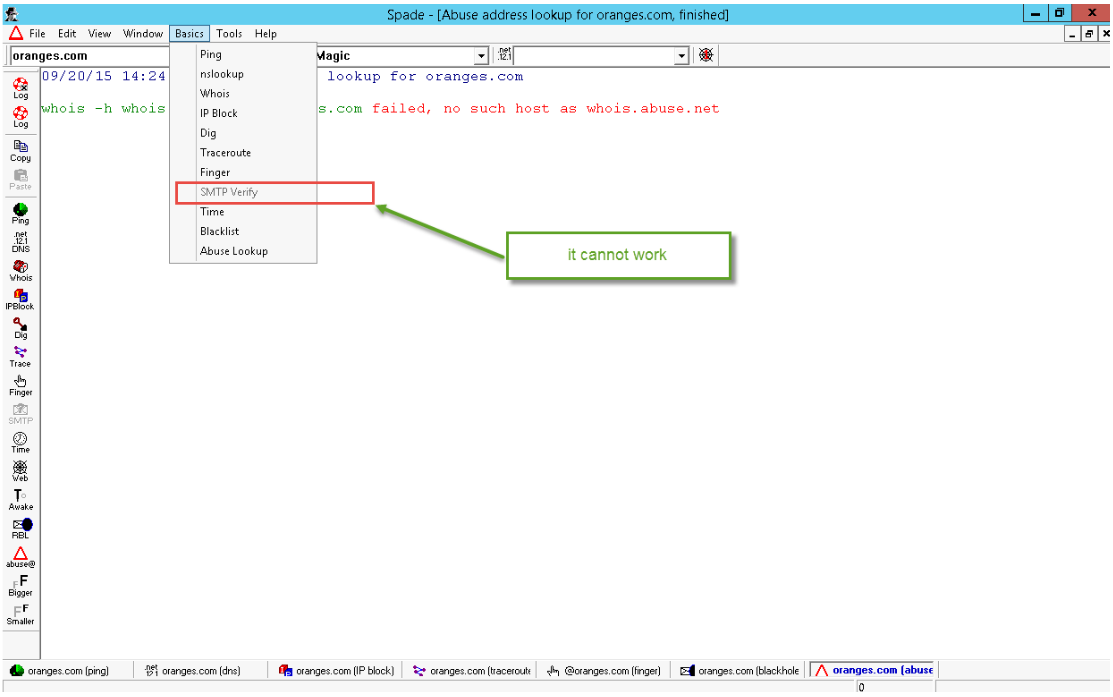
1.4.5 Finger


Spade - [finger @oranges.com, finished]

```
09/20/15 14:17:38 finger @oranges.com
finger @oranges.com (192.168.40.9) ...
failed, couldn't connect to host
```

Description: obtains host/user information from a host running the finger daemon.

1.4.6 SMTP Verify

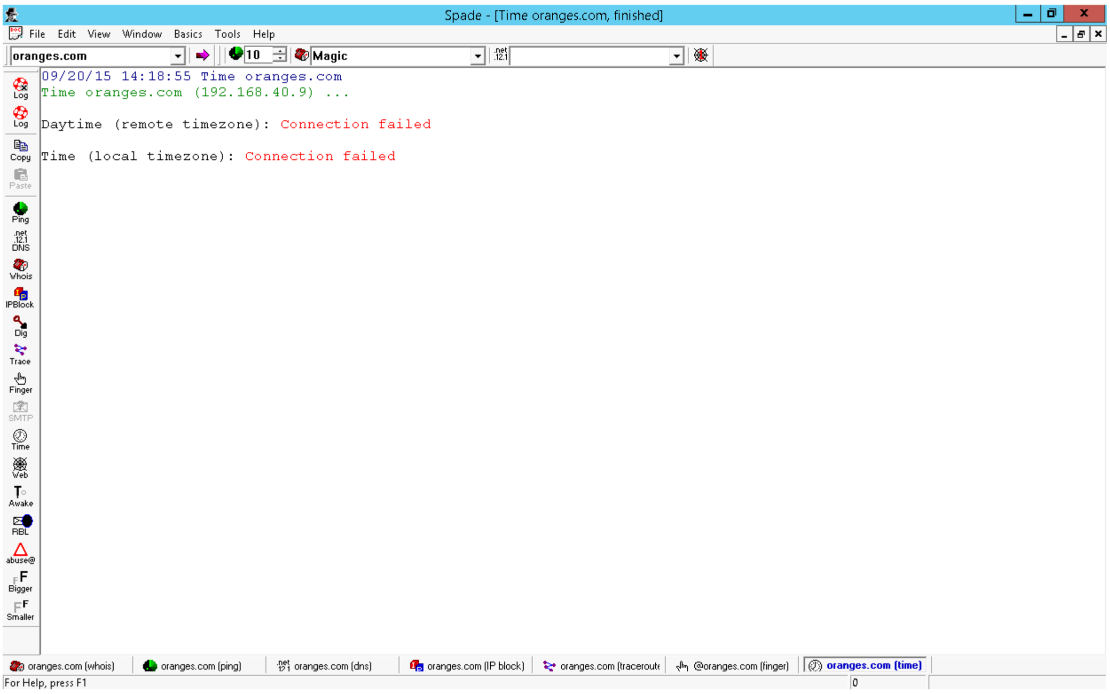

Spade - [Abuse address lookup for oranges.com, finished]

```
09/20/15 14:24                      lookup for oranges.com

whois -h whois                     s.com failed, no such host as whois.abuse.net
```

it cannot work

Description: Used to verify whether an email address is a true address or is being forwarded.

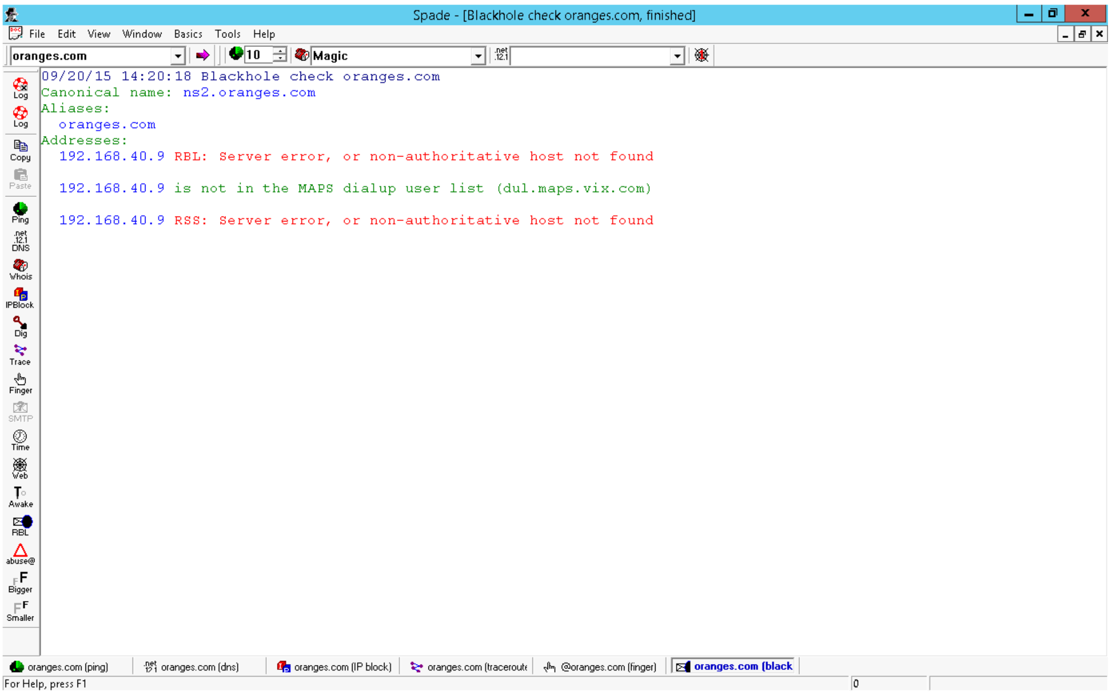
1.4.7 Time



```
09/20/15 14:18:55 Time oranges.com
Time oranges.com (192.168.40.9) ...

Daytime (remote timezone): Connection failed

Time (local timezone): Connection failed
```

Description: return time from server

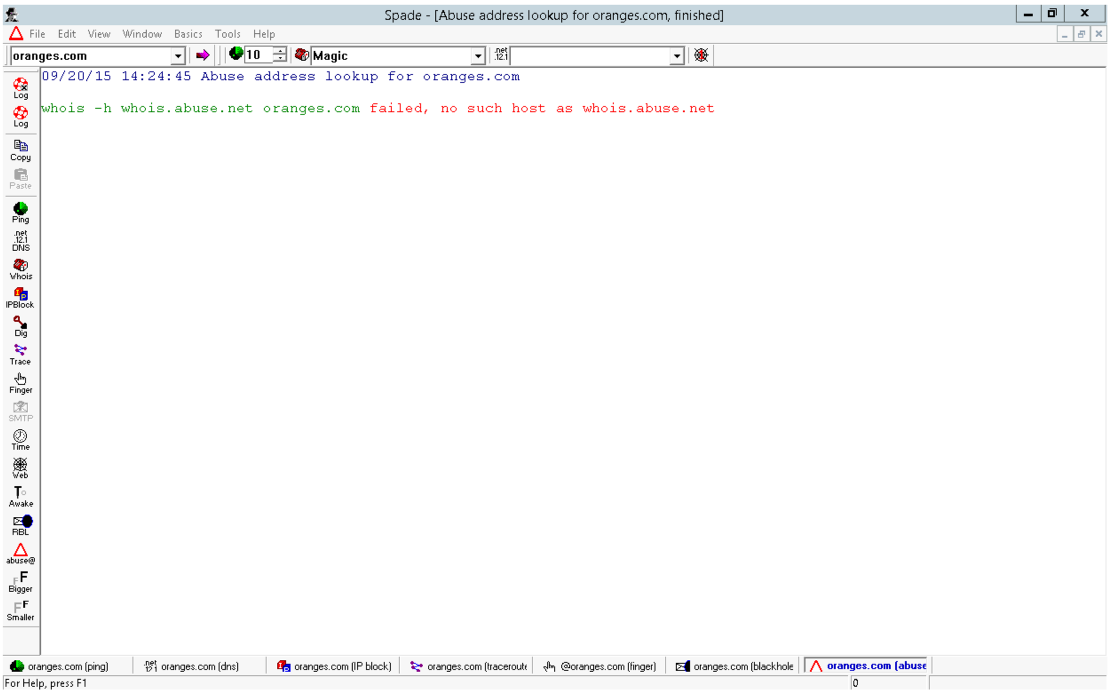
1.4.8 Blacklist



```
09/20/15 14:20:18 Blackhole check oranges.com
Canonical name: ns2.oranges.com
Aliases:
  oranges.com
Addresses:
  192.168.40.9 RBL: Server error, or non-authoritative host not found

  192.168.40.9 is not in the MAPS dialup user list (dul.maps.vix.com)

  192.168.40.9 RSS: Server error, or non-authoritative host not found
```

Description: allow user to check web sites that keep track of known spammers.

1.4.9 Abuse Lookup



```
09/20/15 14:24:45 Abuse address lookup for oranges.com

whois -h whois.abuse.net oranges.com failed, no such host as whois.abuse.net
```

Description: allow user to check web sites that keep track of known spammers.

References:

Microsoft. (2009, 10 13). *Microsoft Security Bulletin MS09-050 - Critical*. Retrieved 9 21, 2005, from technet.microsoft.com: https://technet.microsoft.com/en-us/library/security/ms09-050

SANS Institute InfoSec. (2003). *Using Sam Spade.*