الفصل الاول
جمع معلومات عن الهدف

المؤلف
د.م/ أحمد هاشم الفقي
استشارى أمن المعلومات و التحول الرقمي
Ahmed.Hashem.ElFiky@outlook.com

محتويات هذا الفصل:

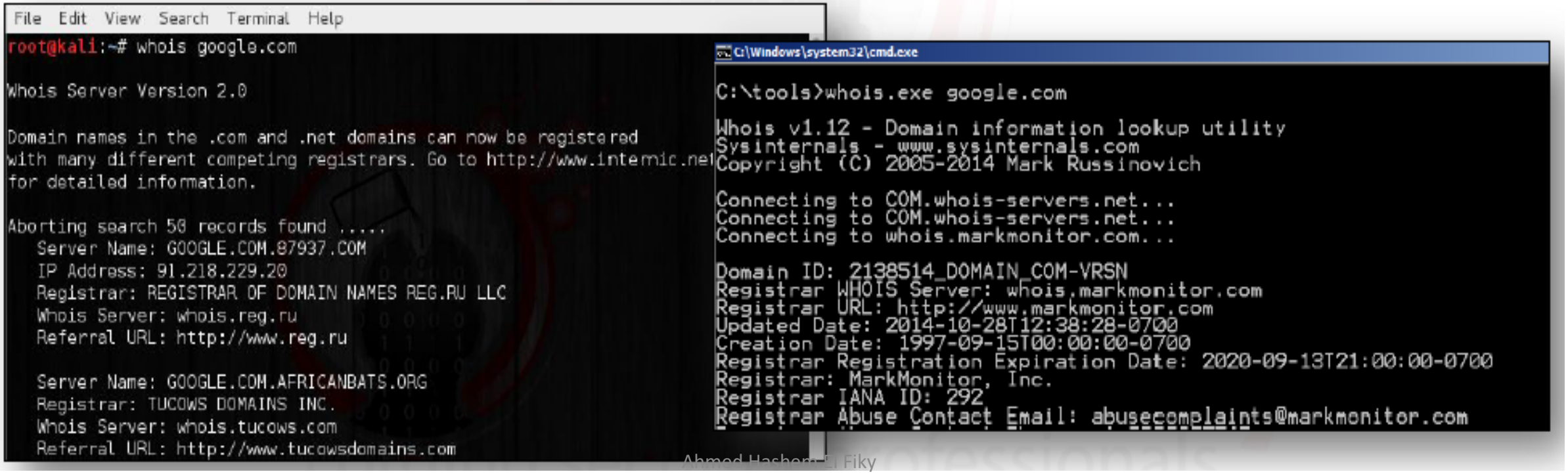
- ما هى أنواع المعلومات التى نسعى لمعرفتها عن الهدف
- فهم ال WHOIS Tool
- فهم ال DNS
- فهم ال nslookup Tool
- فهم موقع Netcraft
- فهم الNetcat Tool
- فهم ال WhatWeb Tool
- فهم ال Wappalyzer Tool
- فهم ال Google Search Operators
- فهم ال dnsrecon Tool
- فهم ال subbrute Tool
- فهم ال theHarvestar Tool
- فهم مصطلح DNS Zone Transfer
- فهم ال fierce Tool
- فهم ال DirBuster Tool
- فهم موقع Shodan HQ
- بناء Functional Graph للهدف

ما هى أنواع المعلومات التى نسعى لمعرفتها عن الهدف

- نسعى لمعرفة بعض المعلومات عن الهدف و منها
  - معلومات عن ال Infrastructure مثلا (Web server, CMS, Database, …)
  - معلومات عن ال Application Logic اى كيفية عمل الهدف
  - معلومات عن ال IPs, Domains and SubDomains
  - معلومات عن ال Virtual hosts

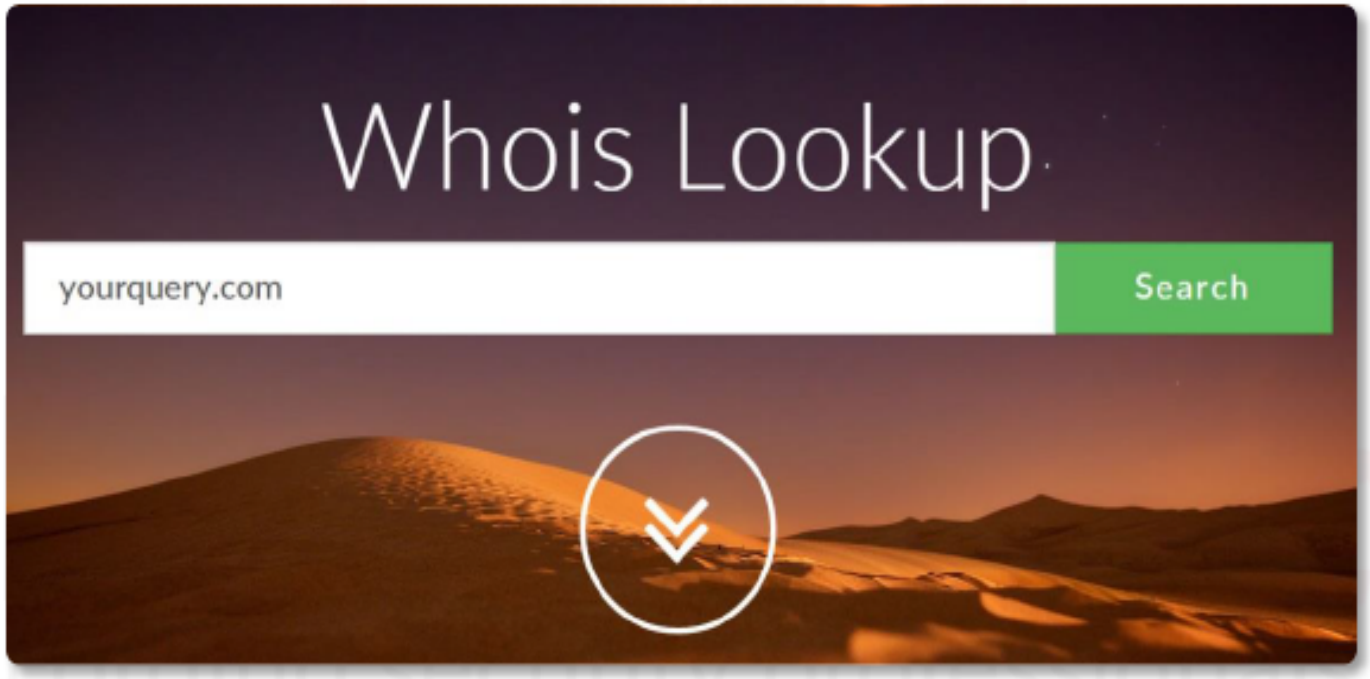
فهم ال WHOIS Tool

- اداة ال WHOIS تبحث عن تفاصيل ownership للهدف من قواعد بيانات مختلفة.
- توجد هذه الاداة فى شكل Command-Based او فى شكل Web-Based



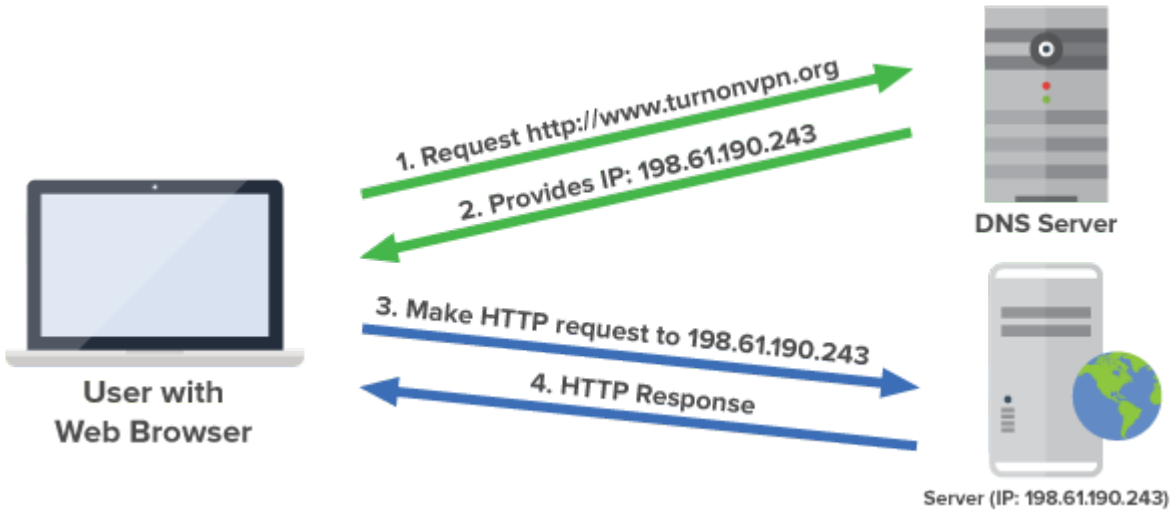
فهم ال WHOIS Tool (تكملة...)

web-based tools such as: whois.domaintools.com



فهم ال DNS

- DNSهو اختصار لمصطلح Domain Name Serviceأو Domain Name System، و يستخدم لربط اسم الدومين الخاص بك لسرفر معين (أي لشركة الاستضافة الخاصة بك).
- وظيفة DNSهنا هي تحويل اسم النطاق أو الدومين الذي يكتبه الزائر في متصفحات الإنترنت، إلى IP Addressيستطيع الكمبيوتر التعامل والاستجابة له.
- كلما قام أحدهم بكتابة اسم النطاق في المتصفح، يقوم DNSفي جزء من الثانية بمطابقة اسم الدومين مع IP Addressالخاص بالموقع، ومن ثم يقوم بجلب البيانات أو تحميل الموقع من السرفر الخاص المخزن عليه بيانات الموقع.



فهم ال DNS (تكمله...)

- يتكون ال DNS من عدة Records منها:
- **A record**
  - يقوم بتوجيه اسم النطاق إلى عنوان IP الخاص بالخادم المستضيف لموقعك.
- **NS record**
  - يشير إلى اسم الخادم المستضيف لموقعك .
- **CNAME record**
  - يستخدم لإنشاء أسماء مستعارة لإسم النطاق الخاص بك. مثلا لديك اسم نطاق domain.com يحمل الموقع الإلكتروني، يمكن عمل اسم نطاق فرعي منه مثل web.domain.com باستخدام CNAME
- **PTR record**
  - ترجمة ال IP address الى اسم ال Domain

فهم ال DNS (تكمله...)

- **MX record**
  - وهو المسؤول عن توجيه البريد الالكتروني حيث يتم تعيين MX record للاشارة إلي خادم البريد الالكتروني علي سبيل المثال

    mail.example.com
  -

Common Resource Record Types

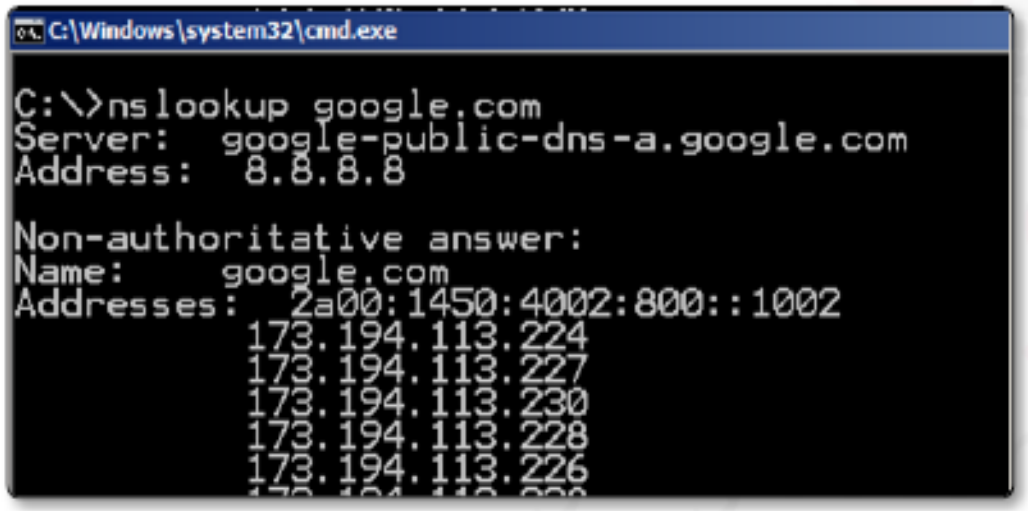
RR Type	Name	Functions
A	Address record	Maps domain name to IP address `www.apnic.net. IN A 203.176.189.99`
AAAA	IPv6 address record	Maps domain name to an IPv6 address `www.apnic.net. IN AAAA 2001:db8::1`
NS	Name server record	Used for delegating zone to a nameserver `apnic.net. IN NS ns1.apnic.net.`
PTR	Pointer record	Maps an IP address to a domain name `99.189.176.203.in-addr.arpa. IN PTR www.apnic.net.`
CNAME	Canonical name	Maps an alias to a hostname `web IN CNAME www.apnic.net.`

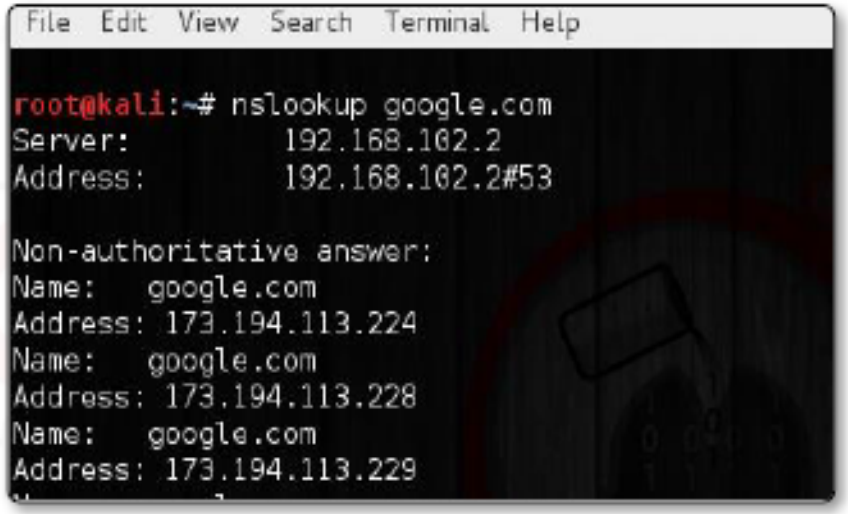
MX	Mail Exchanger	Defines where to deliver mail for user @ domain
		`apnic.net. IN MX 10 mail01.apnic.net.`
		`IN MX 20 mail02.apnic.net.`

فهم ال nslookup Tool

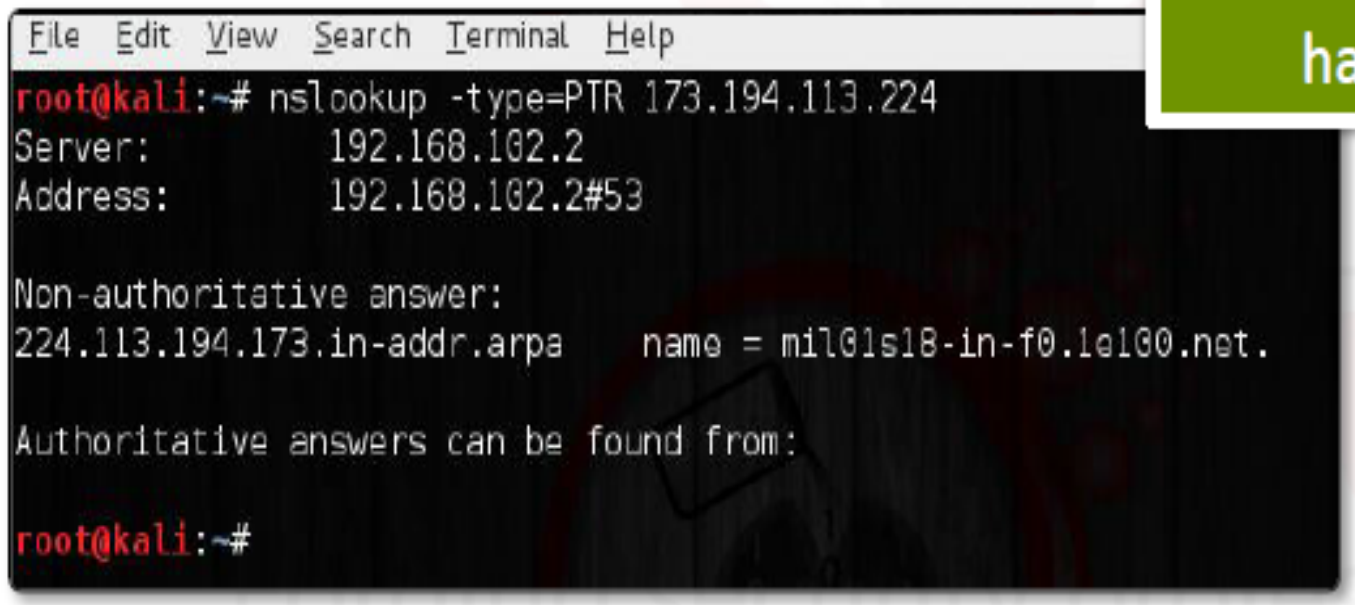
- هى اداة تستخدم لترجمة host name الى IP address و العكس

```
nslookup google.com
```





فهم ال nslookup Tool (تكملة...)



172.194.113.224 is the IP address we have found in the previous step

فهم ال nslookup Tool (تكملة...)

```
nslookup -querytype=ANY google.com
```

فهم ال nslookup Tool (تكملة...)

IP Location	Singapore Singapore Cloudflare Inc.
ASN	AS13335 CLOUDFLARENET - CloudFlare, Inc. (registered J
Whois Server	whois.arin.net
IP Address	104.20.2.47

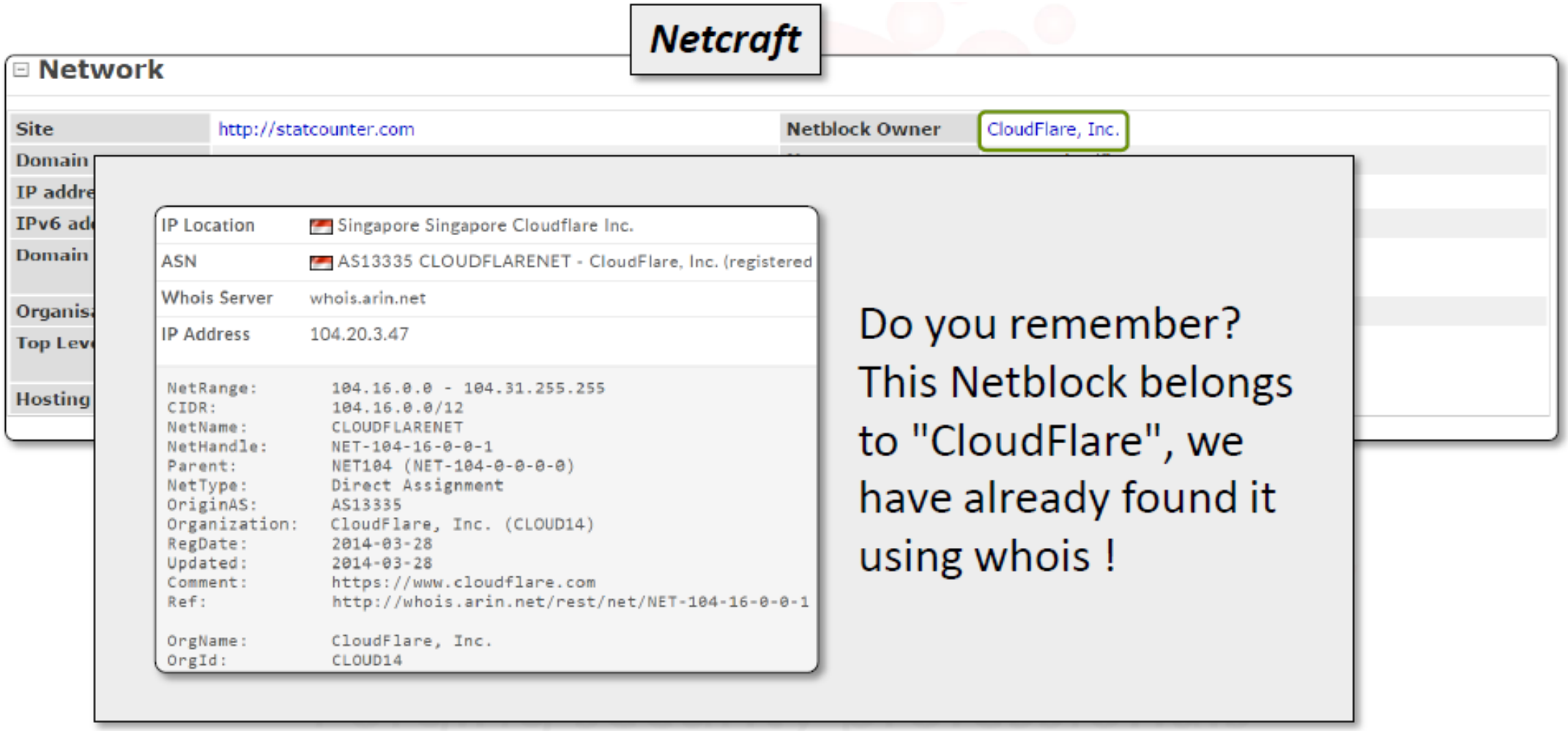
```
NetRange:       104.16.0.0 - 104.31.255.255
CIDR:           104.16.0.0/12
NetName:        CLOUDFLARENET
NetHandle:      NET-104-16-0-0-1
Parent:         NET104 (NET-104-0-0-0-0)
NetType:        Direct Assignment
OriginAS:       AS13335
Organization:   CloudFlare, Inc. (CLOUD14)
RegDate:        2014-03-28
Updated:        2014-03-28
Comment:        https://www.cloudflare.com
Ref:            http://whois.arin.net/rest/net/NET-104-16-0-0-1

OrgName:        CloudFlare, Inc.
OrgId:          CLOUD14
Address:        665 Third Street #207
City:           San Francisco
```

```
root@kali:~# nslookup statcounter.com
Server:         192.168.102.2
Address:        192.168.102.2#53

Non-authoritative answer:
Name:   statcounter.com
Address: 104.20.2.47
Name:   statcounter.com
Address: 104.20.3.47
```

فهم ال Netcraft Tool

- هى اداة غنية بالمعلومات تستخدم كبديل للادوات WHOIS and nslookup وغيرها من المعلومات الهامة

فهم ال Netcraft Tool (تكمله...)



فهم ال Netcraft Tool (تكمله...)

Background

Site title	Microsoft – Official Home Page	**Date first seen**	August 1995
Site rank	1082	**Primary language**	English
Description	At Microsoft our mission and values are to help people and businesses throughout the world realise their full potential.		
Keywords	*Not Present*		

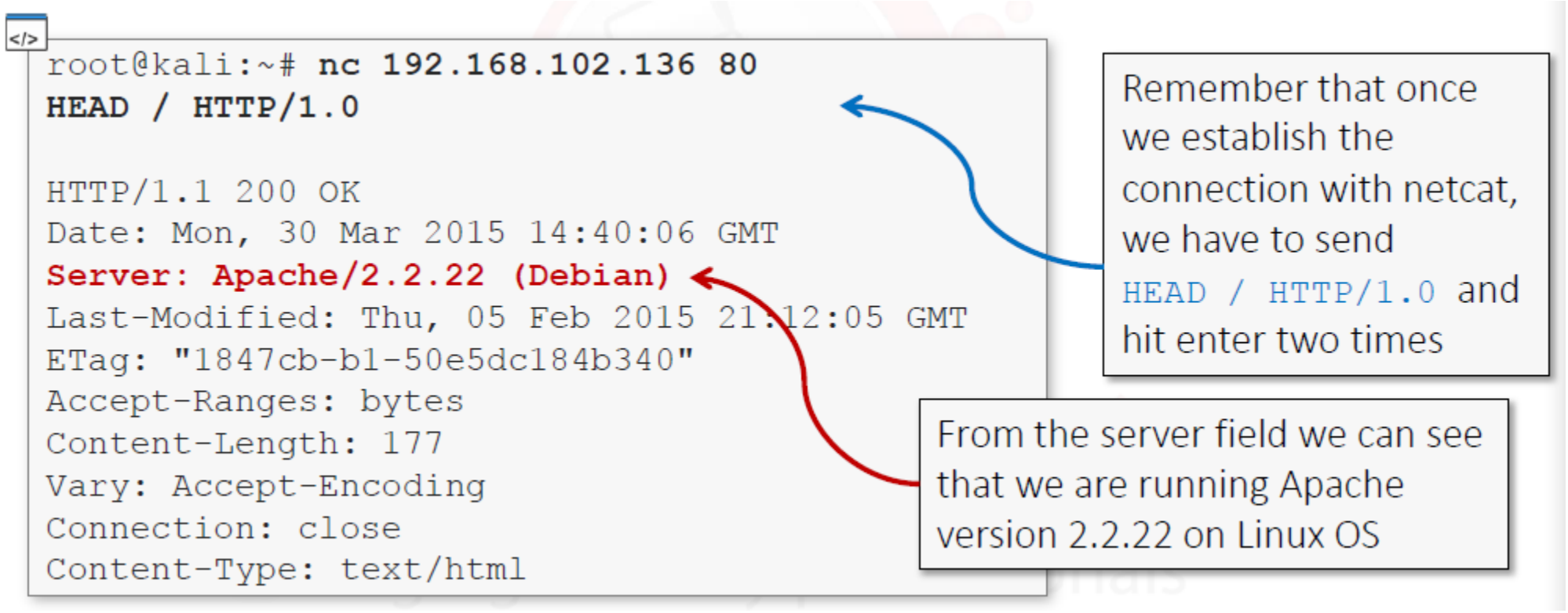
Network

Hosting History

Netblock owner	IP address	OS	Web server	Last seen Refresh
Microsoft Corp One Microsoft Way Redmond WA US 98052	134.170.188.221	unknown	Microsoft-IIS/8.5	29-Mar-2015
Microsoft Corp One Microsoft Way Redmond WA US 98052	134.170.185.46	unknown	Microsoft-IIS/8.5	25-Mar-2015
Microsoft Corp One Microsoft Way Redmond WA US 98052	134.170.188.221	unknown	Microsoft-IIS/8.5	24-Mar-2015
Microsoft Corp One Microsoft Way Redmond WA US 98052	134.170.185.46	unknown	Microsoft-IIS/8.5	22-Mar-2015
Microsoft Corp One Microsoft Way Redmond WA US 98052	134.170.188.221	unknown	Microsoft-IIS/8.5	21-Mar-2015
Microsoft Corp One Microsoft Way Redmond WA US 98052	134.170.185.46	unknown	Microsoft-IIS/8.5	15-Mar-2015
Microsoft Corp One Microsoft Way Redmond WA US 98052	134.170.188.221	unknown	Microsoft-IIS/8.5	14-Mar-2015

فهم ال Netcat Tool

NetCat هي أداة Unix بسيطة جدًا يمكنها قراءة وكتابة اتصالات شبكة TCPأو UDP تم تصميمها كأداة خلفية موثوقة يمكن تشغيلها مباشرة وبسهولة. هنا سوف نستخدمها فى الكشف عن نوع الخادم.



فهم ال Netcat Tool (تكملة...)

```
root@kali:~# nc 134.170.185.46 80
HEAD / HTTP/1.0

HTTP/1.1 301 Moved Permanently
Cache-Control: private
Content-Length: 23
Content-Type: text/html
Location: http://www.microsoft.com
Server: Microsoft-IIS/8.5
Set-Cookie:
ASPSESSIONIDACRQQCDQ=LKKMCDHAFINIAMHBICPIMLJF; path=/
…
```

The following output shows us that the remote Web Server is using IIS version 8.5

فهم ال Netcat Tool (تكملة...)

```
root@kali:~# nc 134.170.188.221 80
HEAD / HTTP/1.0

HTTP/1.1 301 Moved Permanently
..stripped output…
Server: Microsoft-IIS/8.5
X-Powered-By: ASP.NET
X-UA-Compatible: IE=EmulateIE7
Date: Tue, 31 Mar 2015 07:48:01 GMT
Connection: close
```

In this case, the header tells us the Web App is using ASP.NET. Other possible values are PHP, JSP, JBoss and so on.

فهم أداة ال WhatWeb

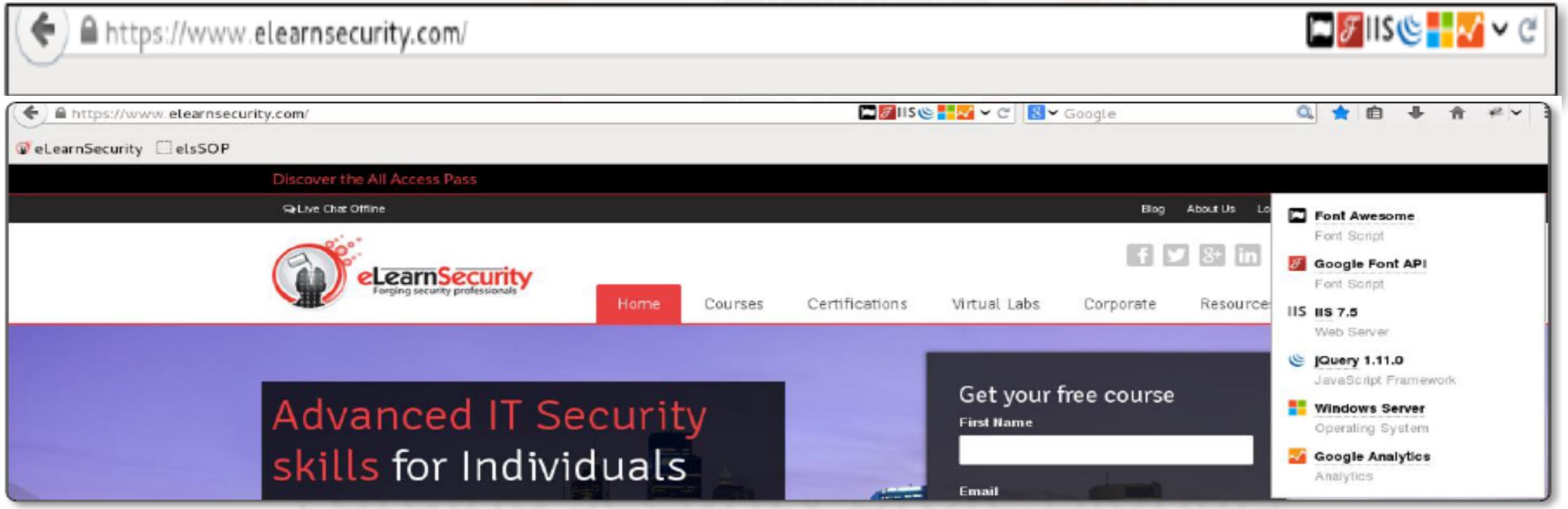
- هى أداة تستخدم ايضا لمعرفة نوع ال Server او الخادم .

```
root@kali:~/tools/WhatWeb# ./whatweb www.elearnsecurity.com
http://www.elearnsecurity.com [302] HTTPServer[Microsoft-IIS/7.5], IP[199.193.116.231],
 Microsoft-IIS[7.5], RedirectLocation[https://www.elearnsecurity.com/], Title[Document
Moved], UncommonHeaders[x-xss-protection,x-frame-options,strict-transport-security], X-
Frame-Options[sameorigin], X-Powered-By[MOS 6502], X-XSS-Protection[1; mode=block]
https://www.elearnsecurity.com/ [200] HTML5, HTTPServer[Microsoft-IIS/7.5], IP[199.193.
116.231], JQuery, Microsoft-IIS[7.5], PoweredBy[eLearnSecurity,], Script[text/javascrip
t], Title[eLearnSecurity - IT Security training courses for individuals and corporation
s], UncommonHeaders[x-xss-protection,x-frame-options,strict-transport-security], X-Fram
e-Options[sameorigin], X-Powered-By[MOS 6502], X-UA-Compatible[IE=edge], X-XSS-Protecti
on[1; mode=block]
root@kali:~/tools/WhatWeb#
```

```
root@kali:~/tools/WhatWeb# ./whatweb -v www.elearnsecurity.com
http://www.elearnsecurity.com/ [302]
http://www.elearnsecurity.com [302] HTTPServer[Microsoft-IIS/7.5], IP[199.193.116.231], Mi
ectLocation[https://www.elearnsecurity.com/], Title[Document Moved], UncommonHeaders[x-xss
ions,strict-transport-security], X-Frame-Options[sameorigin], X-Powered-By[MOS 6502], X-XS
ock]
URL     : http://www.elearnsecurity.com
Status  : 302
   HTTPServer ----------------------------------------------------------------
        Description: HTTP server header string. This plugin also attempts to
                     identify the operating system from the server header.
        String     : Microsoft-IIS/7.5 (from server string)

   IP ------------------------------------------------------------------------
        Description: IP address of the target, if available.
        String     : 199.193.116.231

   Microsoft-IIS -------------------------------------------------------------
        Description: Microsoft Internet Information Services (IIS) for Windows
                     Server is a flexible, secure and easy-to-manage Web server
                     for hosting anything on the Web. From media streaming to
                     web application hosting, IIS's scalable and open
                     architecture is ready to handle the most demanding tasks. -
                     homepage: http://www.iis.net/
        Version    : 7.5

   RedirectLocation ----------------------------------------------------------
        Description: HTTP Server string location. used with http-status 301 and
                     302
        String     : https://www.elearnsecurity.com/ (from location)

   Title ---------------------------------------------------------------------
        Description: The HTML page title
```

فهم أداة ال Wappalyzer

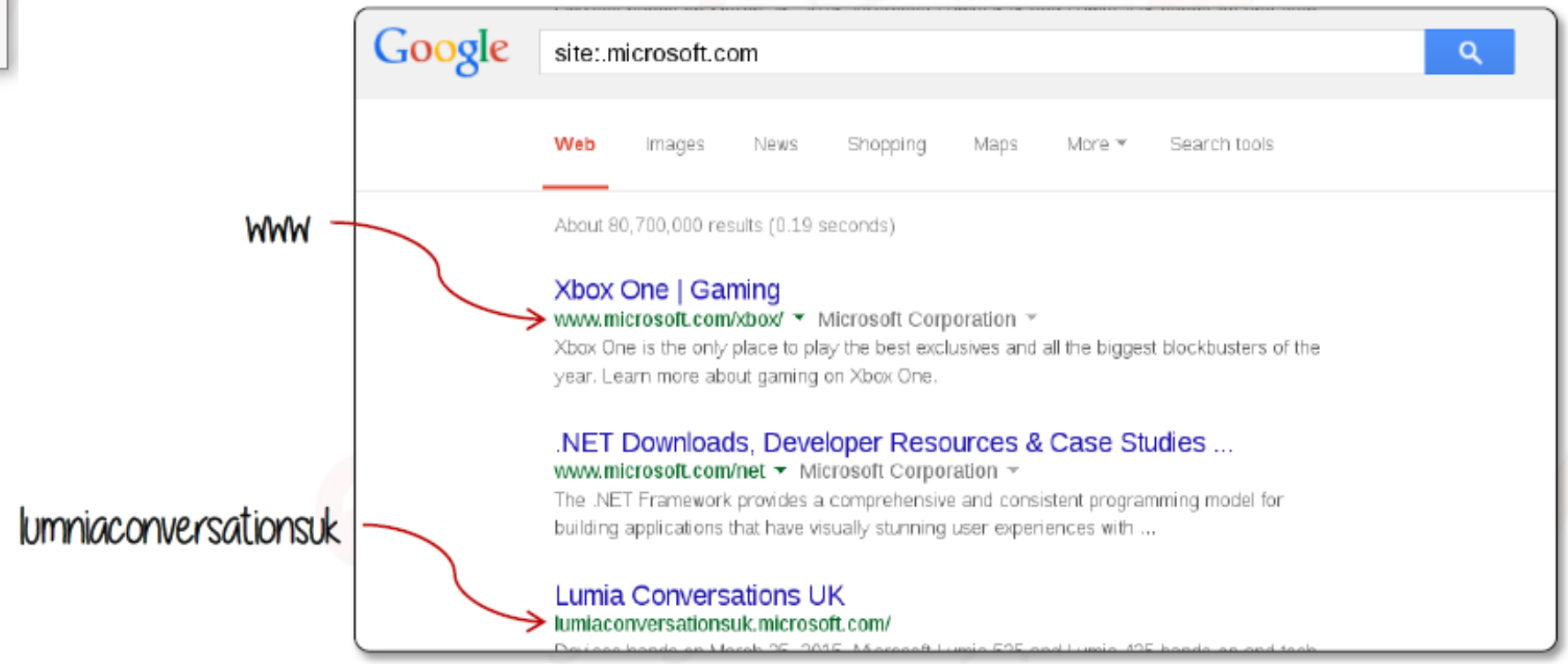
- هى إضافة فى متصفح ال Firefox تستخدم لمعرفة نوع الخادم و لغات البرمجة المستخدمة و معلومات اخرى



فهم أداة ال Google Search Operators

- هى Parameters تستخدم فى موقع جوجل للبحث بشكل اسرع و ادق.

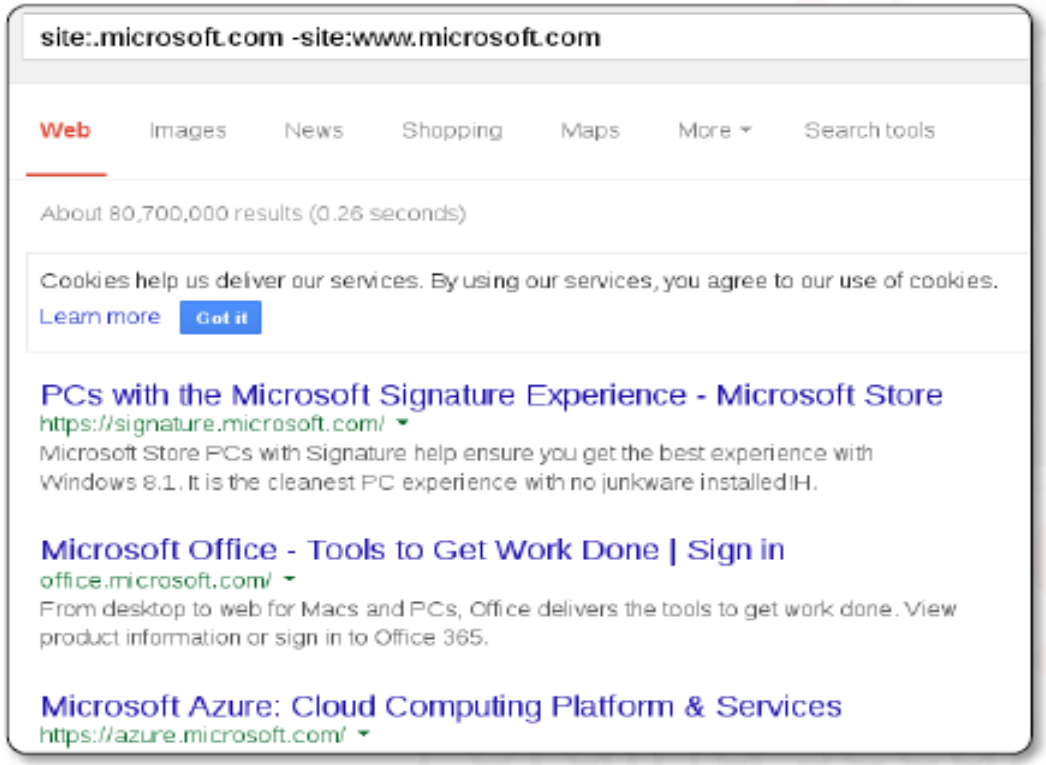
```
site:.microsoft.com
```

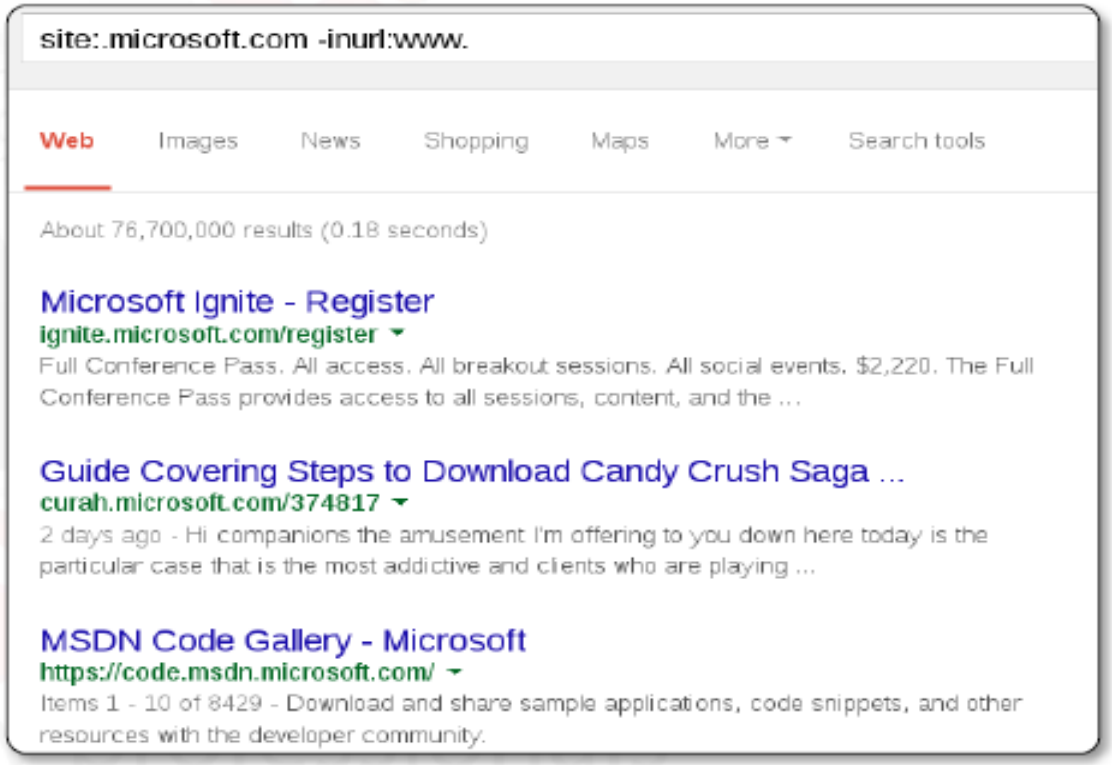


فهم أداة ال Google Search Operators (تكمله ...)

```
site:.microsoft.com -inurl:www.
```

```
site:.microsoft.com -site:www.microsoft.com
```





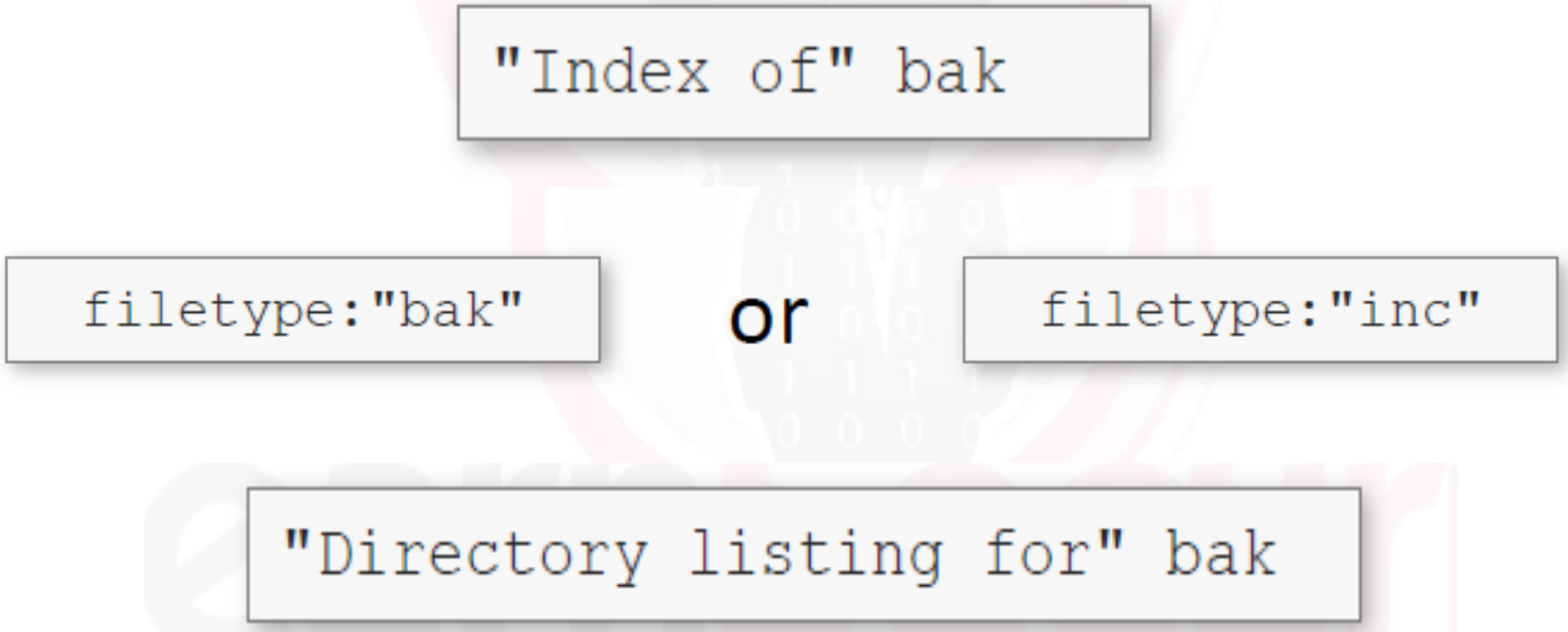
فهم أداة ال Google Search Operators (تكمله ...)

```
site:microsoft.com -site:subdomain1.microsoft.com
-site:subdomain2.microsoft.com -inurl:subdomain3.microsoft.com
```

```
intitle:"Apache HTTP Server" intitle:"documentation"
```

```
intitle:"Apache HTTP Server" intitle:"documentation" site:target.com
```

فهم أداة ال Google Search Operators (تكمله ...)



فهم ال dnsrecon Tool

- هذه الاداة تستخدم للبحث عن ال SubDomains للهدف

```
dnsrecon -d microsoft.com -g
```

```
root@kali:~# dnsrecon -d microsoft.com -g
[*] Performing General Enumeration of Domain: microsoft.com
[-] DNSSEC is not configured for microsoft.com
[*]     SOA ns1.msft.net 208.84.0.53
[*]     SOA ns1.msft.net 2620:0:30::53
[*]     NS ns3.msft.net 193.221.113.53
[*]     NS ns3.msft.net 2620:0:34::53
[*]     NS ns4.msft.net 208.76.45.53
[*]     NS ns4.msft.net 2620:0:37::53
[*]     NS ns1.msft.net 208.84.0.53
[*]     NS ns1.msft.net 2620:0:30::53
[*]     NS ns2.msft.net 208.84.2.53
[*]     NS ns2.msft.net 2620:0:32::53
[*]     MX microsoft-com.mail.protection.outlook.com
[*] Performing Google Search Enumeration
[*]     CNAME www.microsoft.com toggle.www.ms.akadns.net
[*]     CNAME toggle.www.ms.akadns.net www.microsoft.com-c.edgekey.net
[*]     CNAME www.microsoft.com-c.edgekey.net www.microsoft.com-c.edgekey.net.globalredi
[*]     CNAME www.microsoft.com-c.edgekey.net.globalredir.akadns.net e10088.dspb.akamaie
[*]     A e10088.dspb.akamaiedge.net 72.247.197.45
[*]     CNAME ieonline.microsoft.com any.edge.bing.com
[*]     A any.edge.bing.com 204.79.197.200
[*]     CNAME windows.microsoft.com origin.windows.microsoft.com.akadns.net
[*]     A origin.windows.microsoft.com.akadns.net 134.170.119.140
[*]     CNAME support.microsoft.com wildcard.support.microsoft.com.edgekey.net
[*]     CNAME wildcard.support.microsoft.com.edgekey.net e10315.g.akamaiedge.net
[*]     A e10315.g.akamaiedge.net 2.17.104.63
```

فهم ال subbrute Tool

- هذه الاداة تستخدم للبحث عن ال SubDomains للهدف

```
root@kali:~/tools/subbrute# python subbrute.py microsoft.com
microsoft.com
www.microsoft.com
home.microsoft.com
cs.microsoft.com
my.microsoft.com
members.microsoft.com
blogs.microsoft.com
search.microsoft.com
i.microsoft.com
feeds.microsoft.com
forums.microsoft.com
math.microsoft.com
news.microsoft.com
games.microsoft.com
dev.microsoft.com
mail.microsoft.com
info.microsoft.com
music.microsoft.com
support.microsoft.com
help.microsoft.com
s.microsoft.com
e.microsoft.com
office.microsoft.com
profile.microsoft.com
member.microsoft.com
```

```
git clone https://github.com/TheRook/subbrute.git
```

```
python subbrute.py -h
```

```
python subbrute.py -h -s [path_to_file.txt]
```

فهم ال theHarvestar Tool

- هذه الاداة تستخدم للبحث عن ال SubDomains للهدف

```
theharvester [options]
```

-d	Domain to search
-l	Limit the results to work with
-b	Data source (bing, google, linkedin, pgp, all,...)
-f	Output to HTML or XML file (optional - good for long lists)

```
theharvester -d microsoft.com -b google -l 200
-f /root/Desktop/msresults.html
```

Console

```
[+] Emails found:
------------------
oss@microsoft.com
secure@microsoft.com
joakim.karlen@microsoft.com
Edvard.bergstrom@microsoft.com
dinei@microsoft.com
cormac@microsoft.com
@microsoft.com
hiballan@microsoft.com
thomkar@microsoft.com
antr@microsoft.com
simonpj@microsoft.com

[+] Hosts found in search engines:
------------------------------------
[-] Resolving hostnames IPs...
72.247.197.45:www.microsoft.com
134.170.119.140:windows.microsoft.com
168.62.198.20:commerce.microsoft.com
```

HTML

E-mails names found:

- oss@microsoft.com
- secure@microsoft.com
- joakim.karlen@microsoft.com
- Edvard.bergstrom@microsoft.com
- dinei@microsoft.com
- cormac@microsoft.com
- @microsoft.com
- hiballan@microsoft.com
- thomkar@microsoft.com
- antr@microsoft.com
- simonpj@microsoft.com

Hosts found:

- 72.247.197.45:www.microsoft.com
- 134.170.119.140:windows.microsoft.com
- 168.62.198.20:commerce.microsoft.com
- 2.17.104.63:support.microsoft.com
- 191.235.177.147:azure.microsoft.com

```
theharvester -d elearnsecurity.com -b linkedin -l 200
```

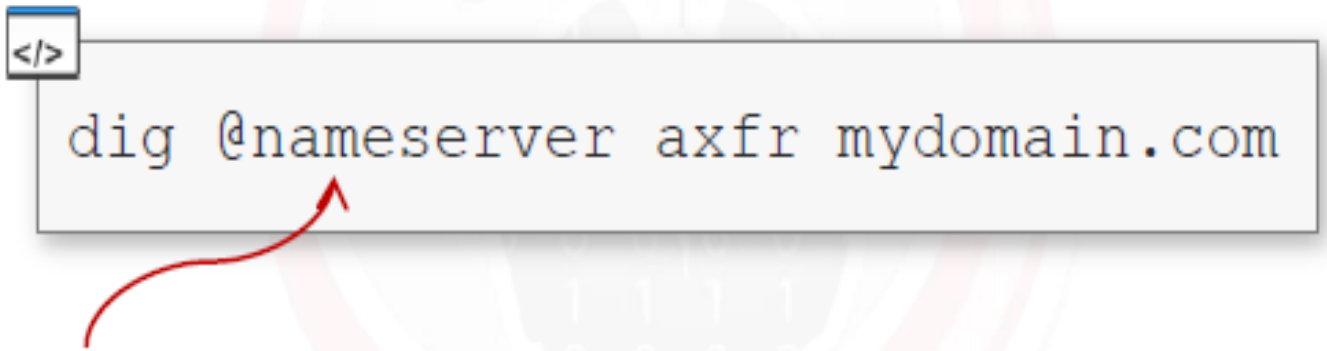
فهم مصطلح DNS Zone Transfer

- يقصد بهذا المصطلح تمرير نسخة من قاعدة البيانات الخاصة ب DNS Server 1 الى DNS Server 2.

```
nslookup -type=NS mydomain.com
```

```
nslookup
server [NAMESERVER FOR mydomain.com]
ls -d mydomain.com
```

```
C:\>nslookup -type=NS elsfoo.com
Server:  google-public-dns-a.google.com
Address:  8.8.8.8

Non-authoritative answer:
elsfoo.com      nameserver = ns.elsfoo.com
elsfoo.com      nameserver = ns6.dnsmadeeasy.com
elsfoo.com      nameserver = ns5.dnsmadeeasy.com
elsfoo.com      nameserver = ns7.dnsmadeeasy.com

C:\>nslookup
Default Server:  google-public-dns-a.google.com
Address:  8.8.8.8

> server ns.elsfoo.com
Default Server:  ns.elsfoo.com
Address:  74.50.103.103

> ls -d elsfoo.com
[ns.elsfoo.com]
 elsfoo.com.                    SOA     ns.elsfoo.com bernyreed.elsfoo.com. (41 900 600 86
 elsfoo.com.                    NS      ns6.dnsmadeeasy.com
 elsfoo.com.                    NS      ns7.dnsmadeeasy.com
 elsfoo.com.                    NS      ns.elsfoo.com
 elsfoo.com.                    NS      ns5.dnsmadeeasy.com
 elsfoo.com.                    MX      5       alt1.aspmx.l.google.com
 elsfoo.com.                    MX      5       alt2.aspmx.l.google.com
 elsfoo.com.                    MX      10      aspmx2.googlemail.com
 elsfoo.com.                    MX      10      aspmx3.googlemail.com
 elsfoo.com.                    MX      1       aspmx.l.google.com
 elsfoo.com.                    TXT             "google-site-verification=omyr9Nazb1WYCs_
axvvtCjTI2EA4_S-Q"

 elsfoo.com.                    TXT             "v=spf1 include:_spf.google.com ~all"

 ns6.dnsmadeeasy.com.           A       208.80.124.13
 ns7.dnsmadeeasy.com.           A       208.80.126.13
 ns5.dnsmadeeasy.com.           A       208.94.148.13
 ns5.dnsmadeeasy.com.           AAAA    2600:1800:5::1
 admin                          A       74.50.103.103
 intranet                       A       74.50.103.103
 ns                             A       74.50.103.103
 private                        A       74.50.103.103
 www                            A       74.50.103.103
 elsfoo.com.                    SOA     ns.elsfoo.com bernyreed.elsfoo.com. (41 900 600 86
>
```



- nameserver is a nameserver for mydomain.com
- axfr is the mnemonic opcode for the DNS zone transfer.

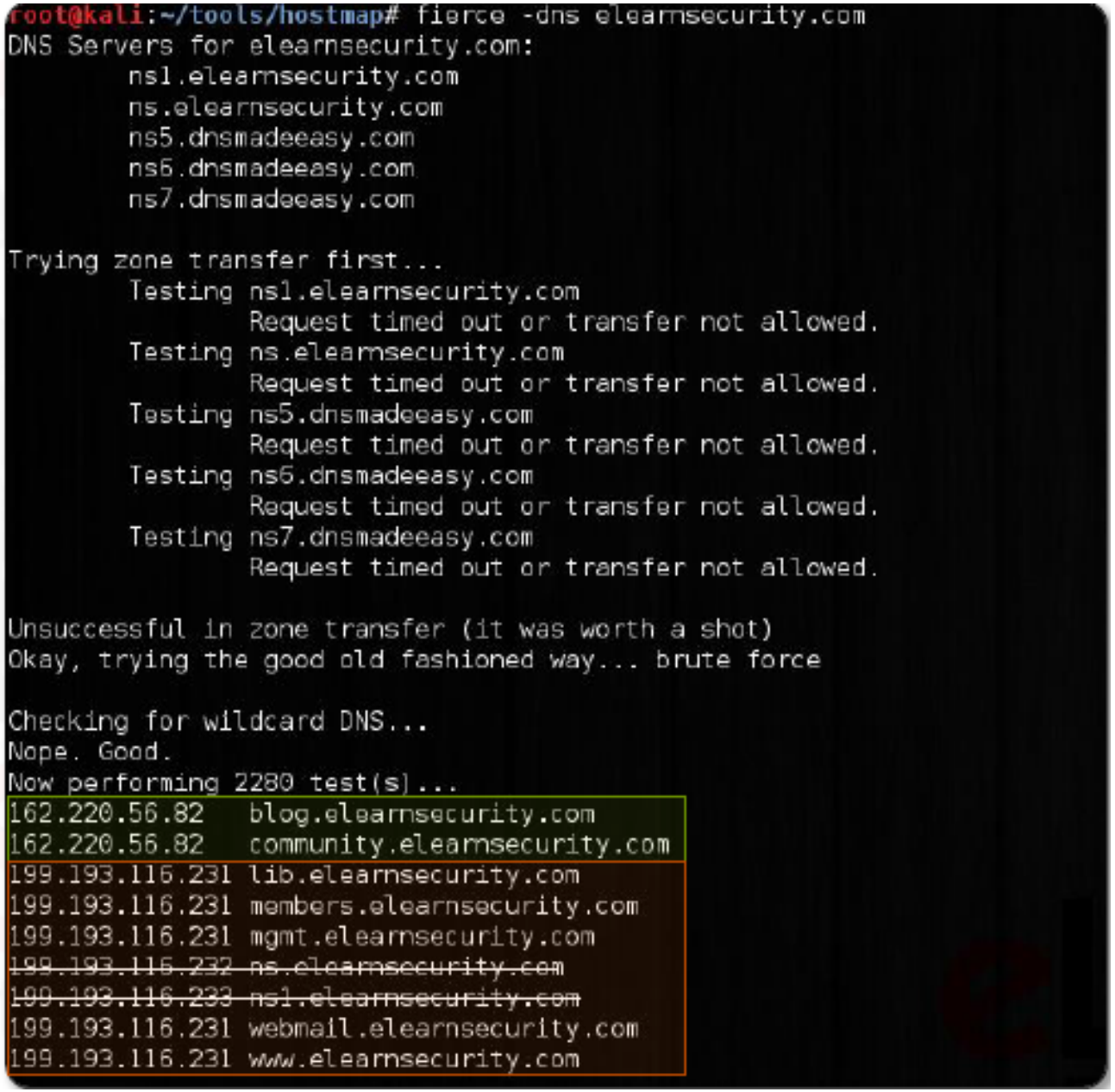
```
root@kali:~# dig @ns.elsfoo.com AXFR elsfoo.com

; <<>> DiG 9.8.4-rpz2+rl005.12-P1 <<>> @ns.elsfoo.com AXFR elsfoo.com
; (1 server found)
;; global options: +cmd
elsfoo.com.             3600    IN      SOA     ns.elsfoo.com. bernyreed.elsfoo.com. 41 900 600 8640
elsfoo.com.             3600    IN      NS      ns6.dnsmadeeasy.com.
elsfoo.com.             3600    IN      NS      ns7.dnsmadeeasy.com.
elsfoo.com.             3600    IN      NS      ns.elsfoo.com.
elsfoo.com.             3600    IN      NS      ns5.dnsmadeeasy.com.
elsfoo.com.             3600    IN      MX      5 alt1.aspmx.l.google.com.
elsfoo.com.             3600    IN      MX      5 alt2.aspmx.l.google.com.
elsfoo.com.             3600    IN      MX      10 aspmx2.googlemail.com.
elsfoo.com.             3600    IN      MX      10 aspmx3.googlemail.com.
elsfoo.com.             3600    IN      MX      1 aspmx.l.google.com.
elsfoo.com.             3600    IN      TXT     "google-site-verification=omyr9Nazb1WYCs_DW29VGj_zMJ
elsfoo.com.             3600    IN      TXT     "v=spf1 include:_spf.google.com -all"
ns6.dnsmadeeasy.com.    3600    IN      A       208.80.124.13
ns7.dnsmadeeasy.com.    3600    IN      A       208.80.126.13
ns5.dnsmadeeasy.com.    3600    IN      A       208.94.148.13
ns5.dnsmadeeasy.com.    3600    IN      AAAA    2600:1800:5::1
admin.elsfoo.com.       3600    IN      A       74.50.103.103
intranet.elsfoo.com.    3600    IN      A       74.50.103.103
ns.elsfoo.com.          3600    IN      A       74.50.103.103
private.elsfoo.com.     3600    IN      A       74.50.103.103
www.elsfoo.com.         3600    IN      A       74.50.103.103
elsfoo.com.             3600    IN      SOA     ns.elsfoo.com. bernyreed.elsfoo.com. 41 900 600 8640
;; Query time: 144 msec
;; SERVER: 74.50.103.103#53(74.50.103.103)
;; WHEN: Tue Mar 31 12:01:01 2015
;; XFR size: 22 records (messages 1, bytes 800)
```

فهم ال Virtual Hosts

Virtual Hosts = Shared Hosting Environment

- حيث الخادم الذى له IP address واحد يحمل اكثر من موقع / host

Here for example there are multiple virtual hosts associated to the IP address 192.168.3.2.

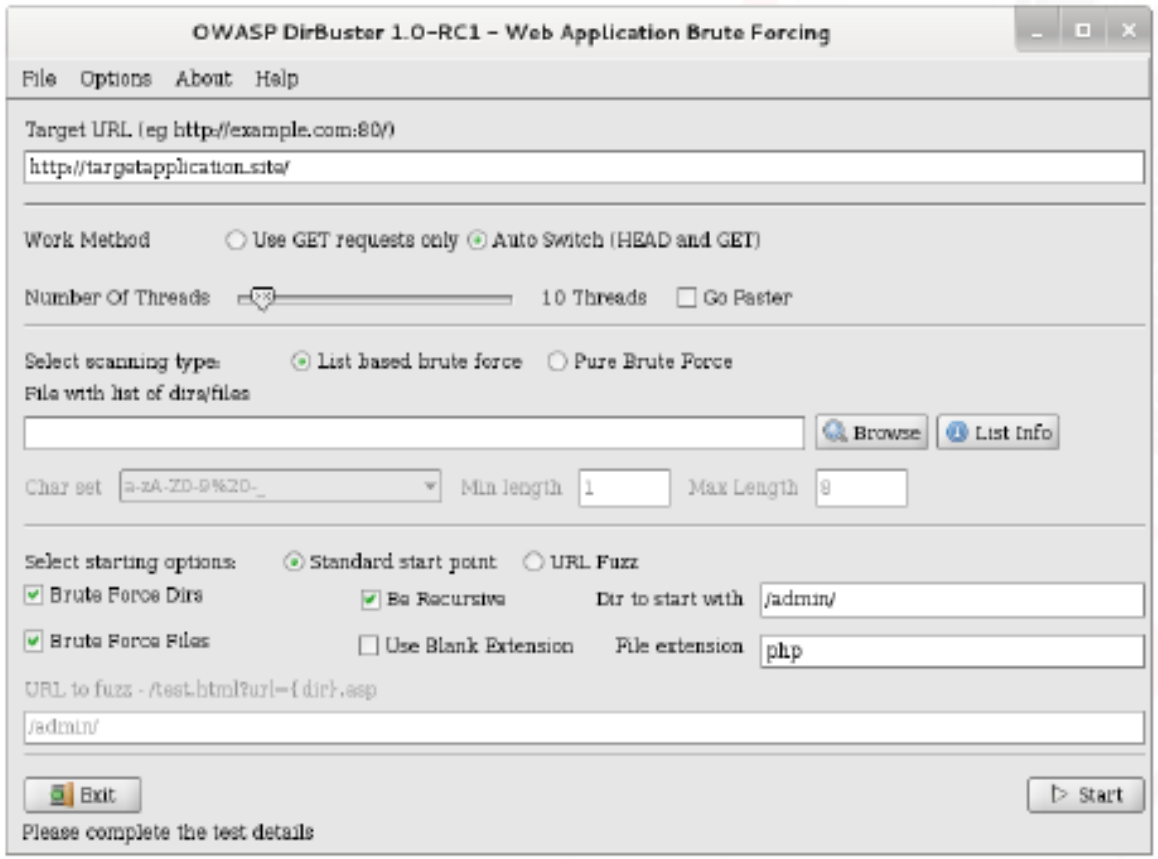


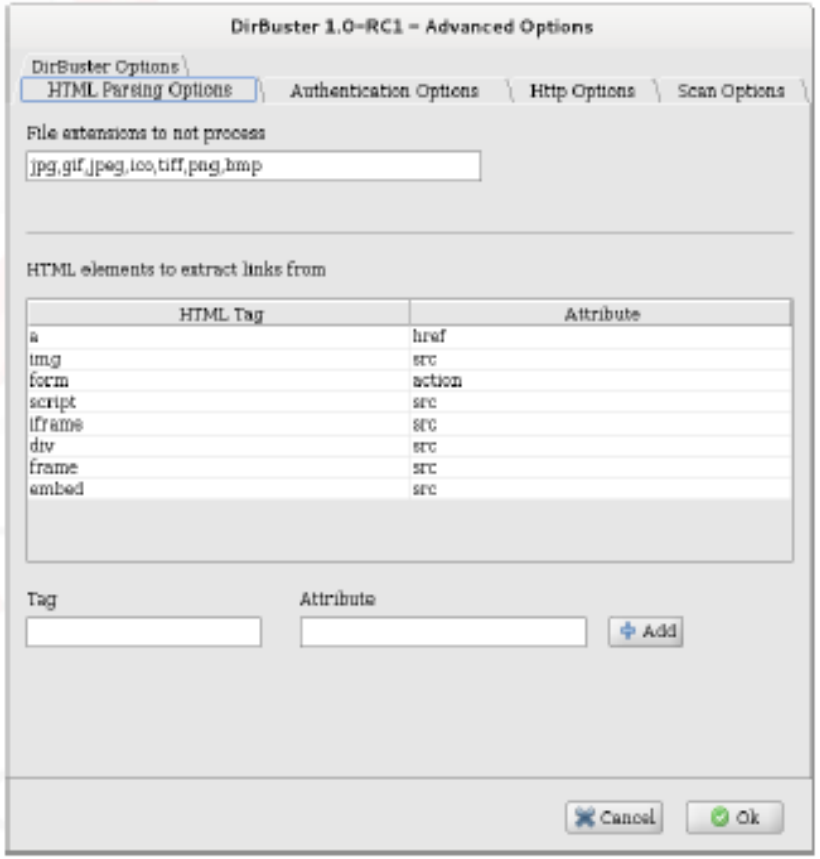
فهم أداة ال Fierce

- تستخدم هذه الاداة لمعرفة ال Virtual Hosts اللى على نفس ال IP address

فهم ال DirBuster Tool

- هى أداة تستخدم لاكتشاف الملفات المخية فى الموقع.





فهم موقع Shodan HQ

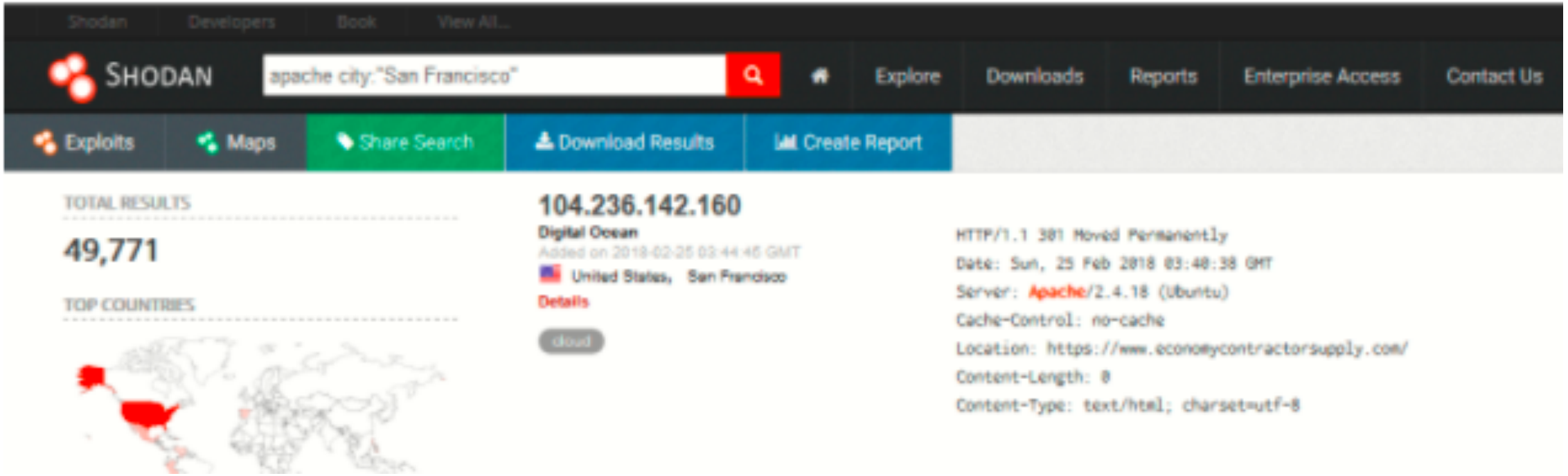
- هو موقع يستخدم لجمع المعلومات عن الهدف من نوع الخادم و ال Ports المفتوحة علية و غيرها من المعلومات الهامة.

Shodan searches includes the following protocols

- HTTP(S)
- SSH
- SNMP
- MySQL / MondoDB
- RDP
- FTP
- Telnet
- and few more

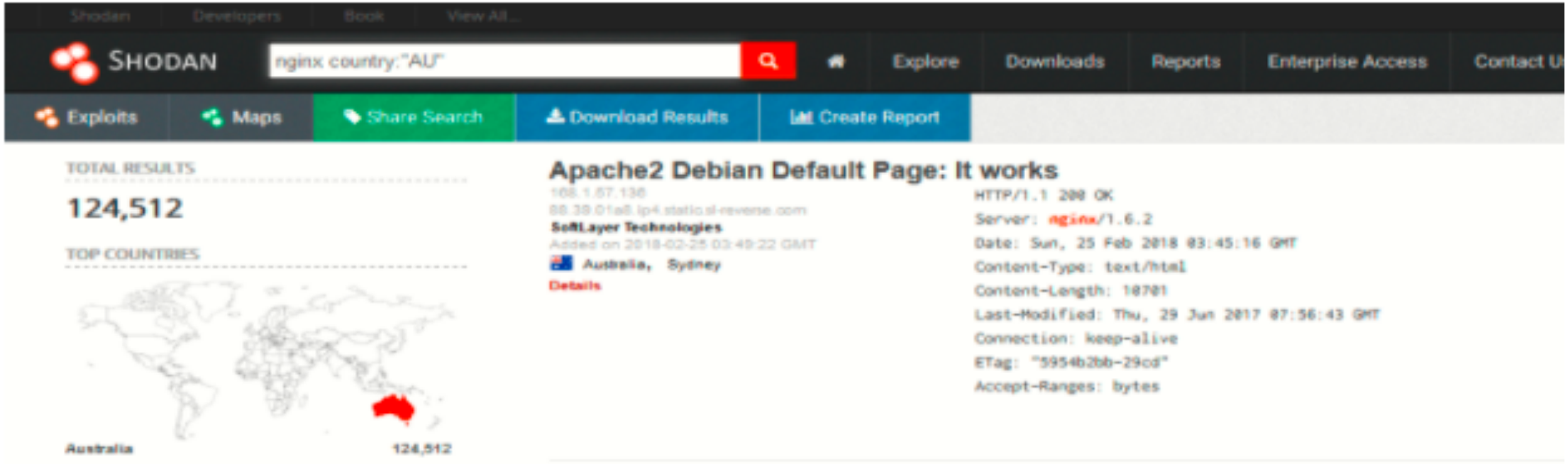
1. Find Apache servers in San Francisco:

> apache city:"San Francisco"



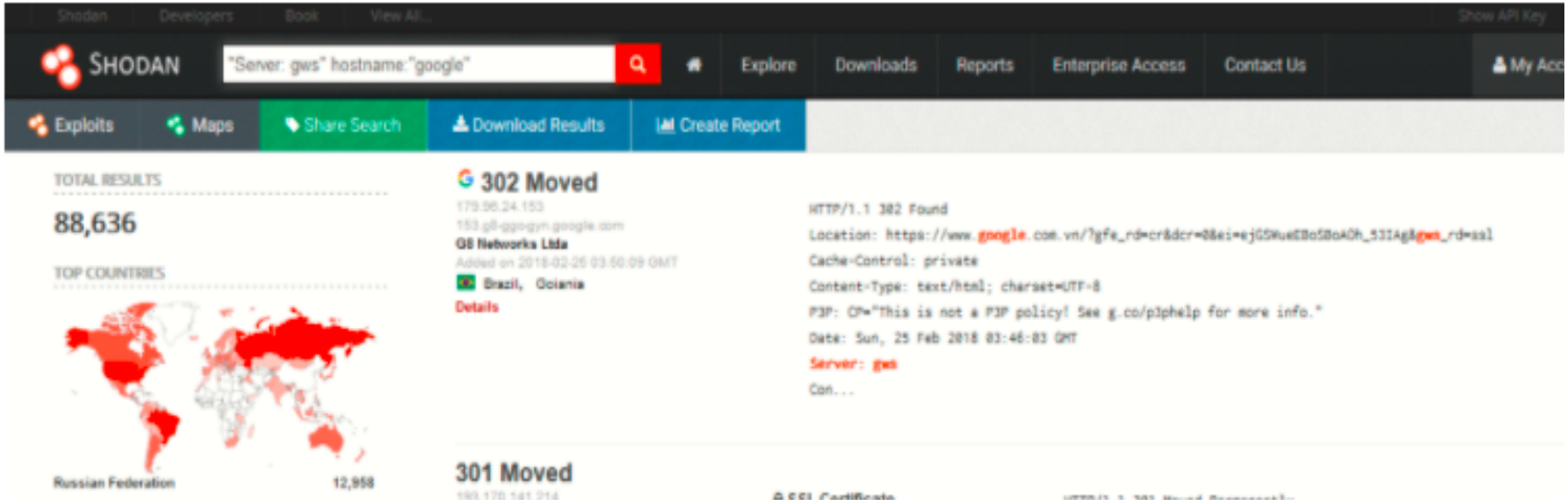
2. Find Nginx servers in Australia:

> nginx country:"AU"



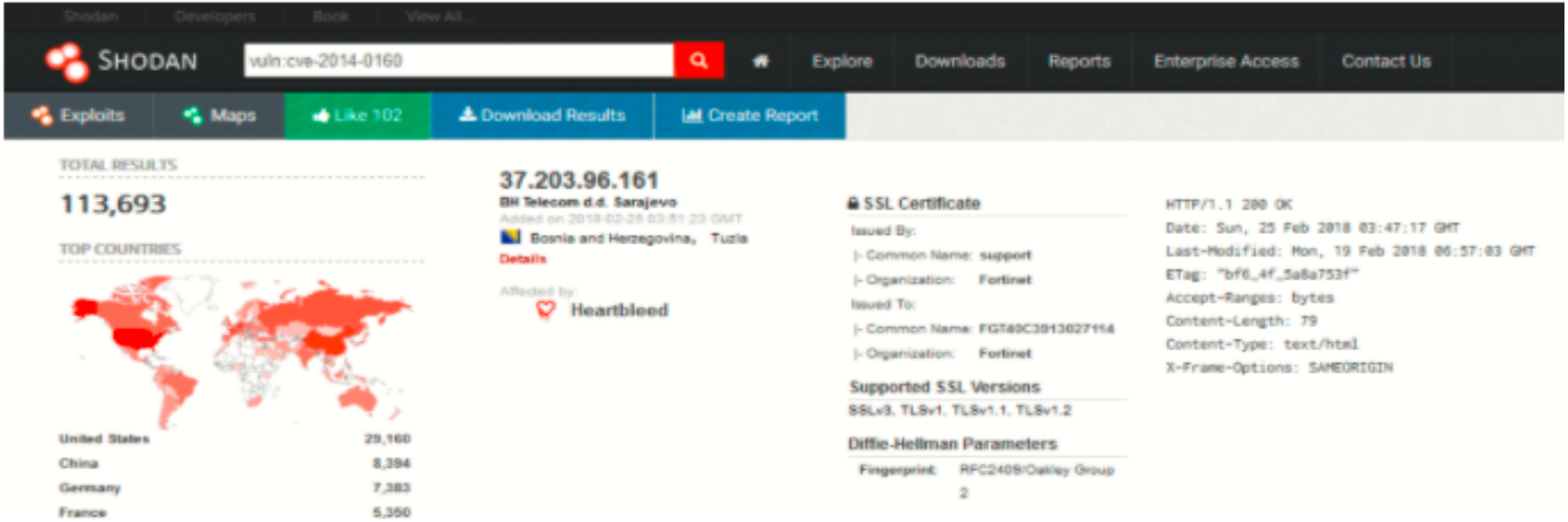
3. Find GWS (Google Web Server) servers:

> "Server: gws" hostname:"google"



4. Search with CVE ID

> vuln:cve-2014-0160



Here are some other basic filters which you can easily use with Shodan:

- **city:** find devices in a particular city
- **country:** find devices in a particular country
- **geo:** you can pass it coordinates
- **hostname:** find values that match the hostname
- **net:** search based on an IP or /x CIDR
- **os:** search based on operating system
- **port:** find particular ports that are open
- **before/after:** find results within a timeframe

For Webcams –

- **Code:** Server: SQ-WEBCAM
- **Link –** https://www.shodan.io/search?query=Server%3A+SQ-WEBCAM

For Cams –

- **Code:** linux upnp avtech
- **Link –** https://www.shodan.io/search?query=linux+upnp+avtech

For Netcam –

- **Code:** netcam
- **Link –** https://www.shodan.io/search?query=netcam

For Default Passwords –

- **Code:** "default password"
- **Link –** https://www.shodan.io/search?query=%22default+password%22

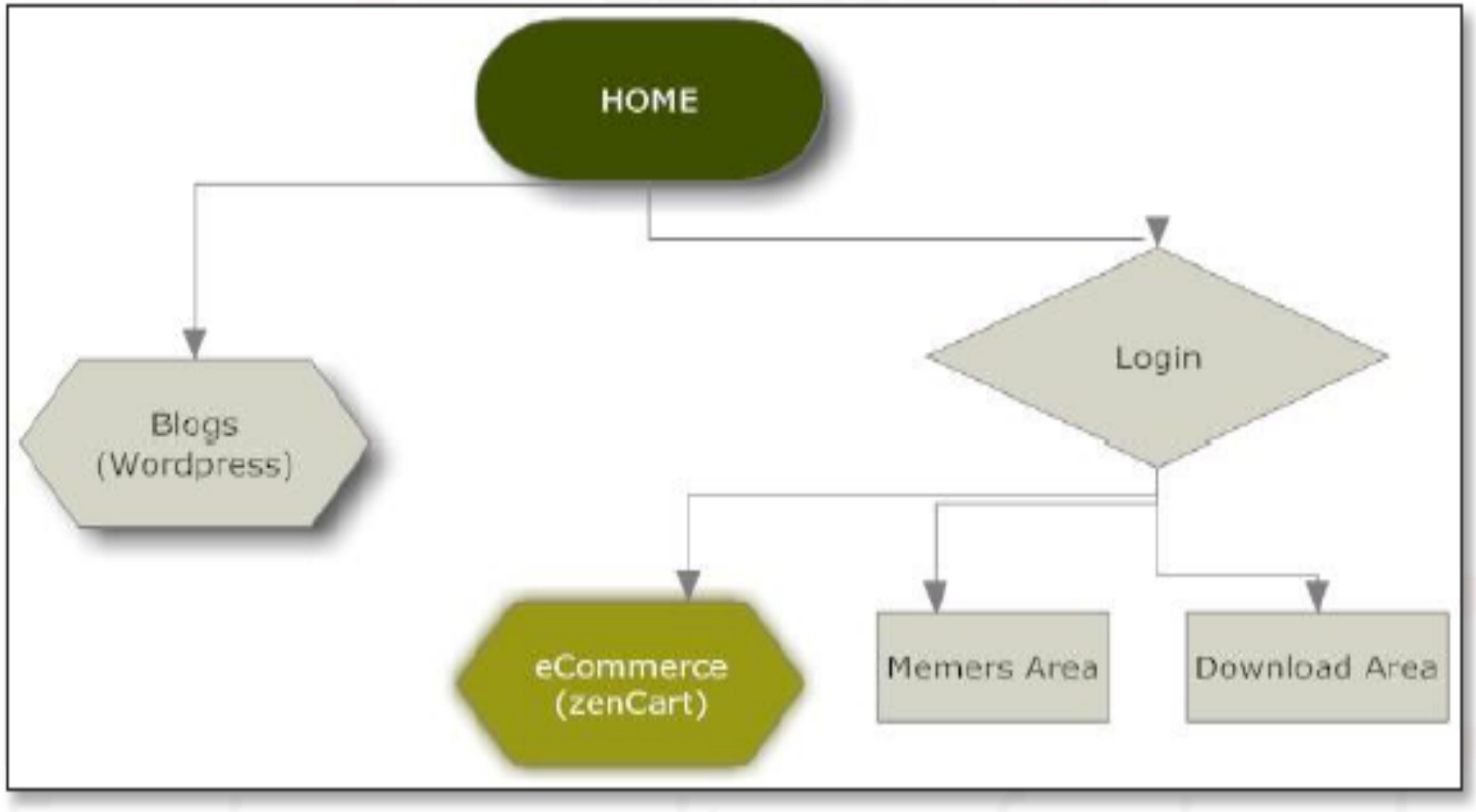
بناء Functional Graph للهدف

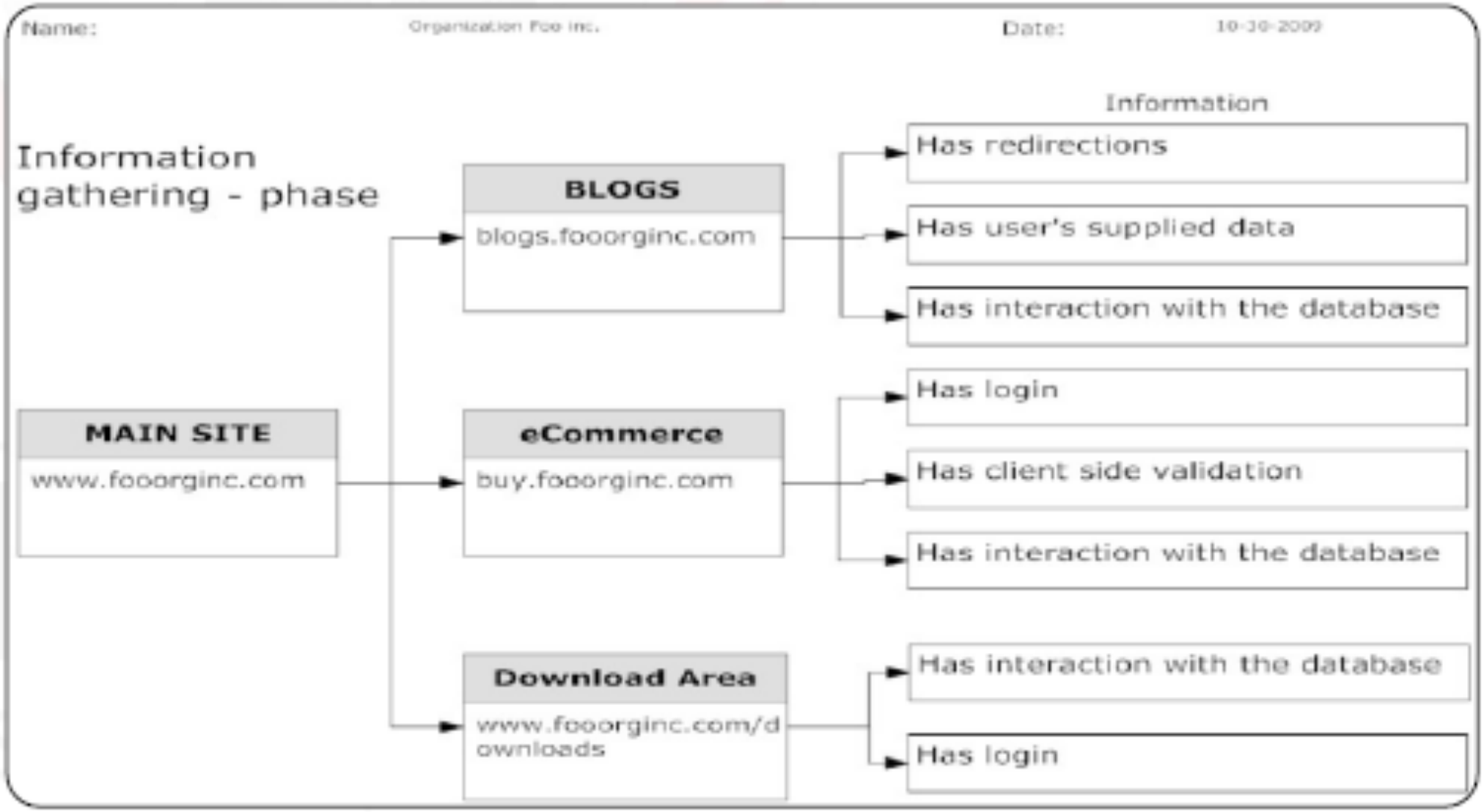
Our first step in this case will be to consider the overall scope of the application:

- What is it for?
- Does it allow user registration?
- Does it have an administration panel?
- Does it take input from the user?
- What kind of input?
- Does it accept file uploads?
- Does it use JavaScript or Ajax or Flash? And so on.

The following questions should help guide you:

- What is the purpose of the website/web application?
  - Sell online?
  - Corporate online presence?
  - Blogging?
- What seems to be the core of the website?
  - Selling products?
  - Do they sell memberships? digital contents?
- Does it require login to perform certain actions?
- What are the main areas of the website?
  - Blogs?
  - eCommerce area?


HOME
Blogs
(Wordpress)
Login
eCommerce
(zenCart)
Memers Area
Download Area


Name:
Organization Foo inc.
Date:
10-10-2009
Information gathering - phase
Information
MAIN SITE
www.fooorginc.com
BLOGS
blogs.fooorginc.com
eCommerce
buy.fooorginc.com
Download Area
www.fooorginc.com/downloads
Has redirections
Has user's supplied data
Has interaction with the database
Has login
Has client side validation
Has interaction with the database
Has interaction with the database
Has login

تم بحمد الله انتهاء الفصل الاول