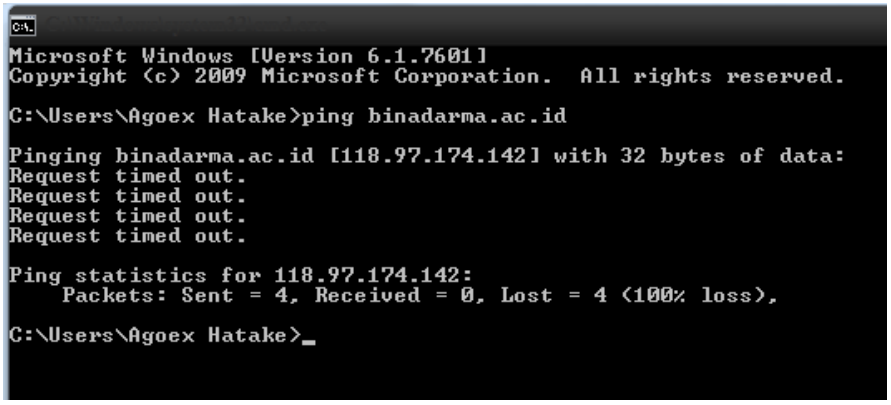
Nama : Leny Novita Sari
NIM : 09011181320027
Keamanan Jaringan Komputer

Reconnaissance

Reconnaissance merupakan tahap persiapan yang digunakan untuk mengumpulkan informasi lebih lanjut. Mengumpulkan informasi termasuk menemukan beberapa informasi dasar yang berguna, seperti alamat IP, topologi jaringan, sumber daya jaringan dan bahkan informasi pribadi tentang pengguna yang dapat digunakan pada langkah berikutnya. Search engine biasanya digunakan untuk memperoleh informasi dari sumber online, saat offline pengumpulan informasi didapatkan dengan membawa potongan informasi yang tersebar ditambah dengan rekayasa sosial untuk mengkonsolidasikan sejumlah besar data yang dapat digunakan untuk melakukan pengintaian dari lingkungan target. Rekayasa sosial adalah salah satu cara termudah untuk penyusup mendapatkan akses tidak sah pada target yang sengaja dipilih.

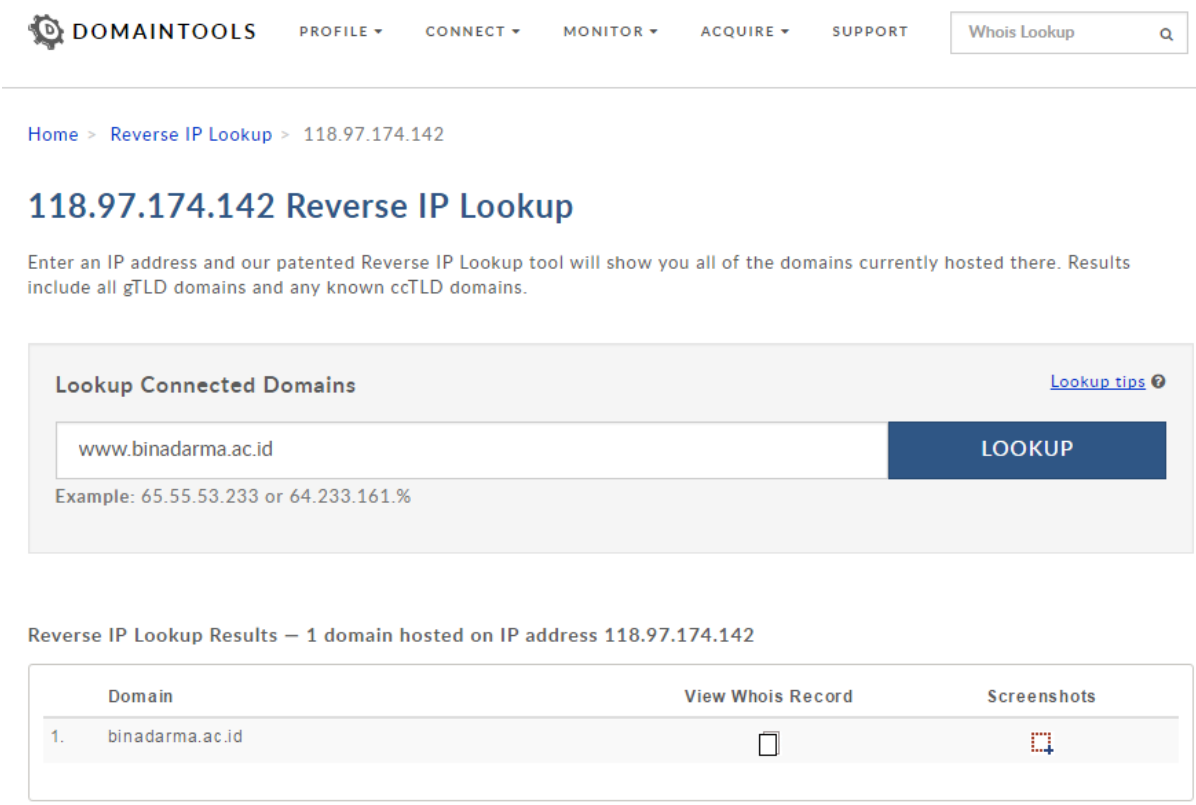
Target : binadarma.ac.id

Langkah pertama yang dilakukan adalah ping target untuk mendapatkan informasi berupa alamat IP target, waktu round trip dan lain sebagainya.



Gambar.1 Hasil Ping Domain Target

Setelah mendapatkan alamat IP target, kita coba untuk mereverse IP yang bertujuan untuk memetakan IP target yang kita dapatkan kepada sebuah domain, dalam artian kita dapat mengecek kesesuaian IP yang kita dapatkan dengan domain target yang dipilih.



Gambar.2 Reverse IP

Jika sudah sesuai, gunakan tools whois seperti : http://whois.domaintools.com, http://bgp.he.net, www.robtex.com dan tools lainnya, untuk memulai mengumpulkan informasi seperti alamat IP, topologi jaringan, sumber daya jaringan dan bahkan informasi pribadi tentang pengguna.

Whois & Quick Stats

Email	suryayusra@binadarma.ac.id is associated with ~2 domains
Registrant Org	Darma is associated with ~34 other domains
Dates	Created on 2001-08-07 - Expires on 2017-10-31 - Updated on 2016-10-24
IP Address	118.97.174.142 is hosted on a dedicated server
IP Location	- Riau - Batam - Pt Telkom Indonesia
ASN	AS17974 TELKOMNET-AS2-AP PT Telekomunikasi Indonesia, ID (registered Oct 08, 2001)
Whois History	275 records have been archived since 2009-10-23
Whois Server	whois.pandi.or.id

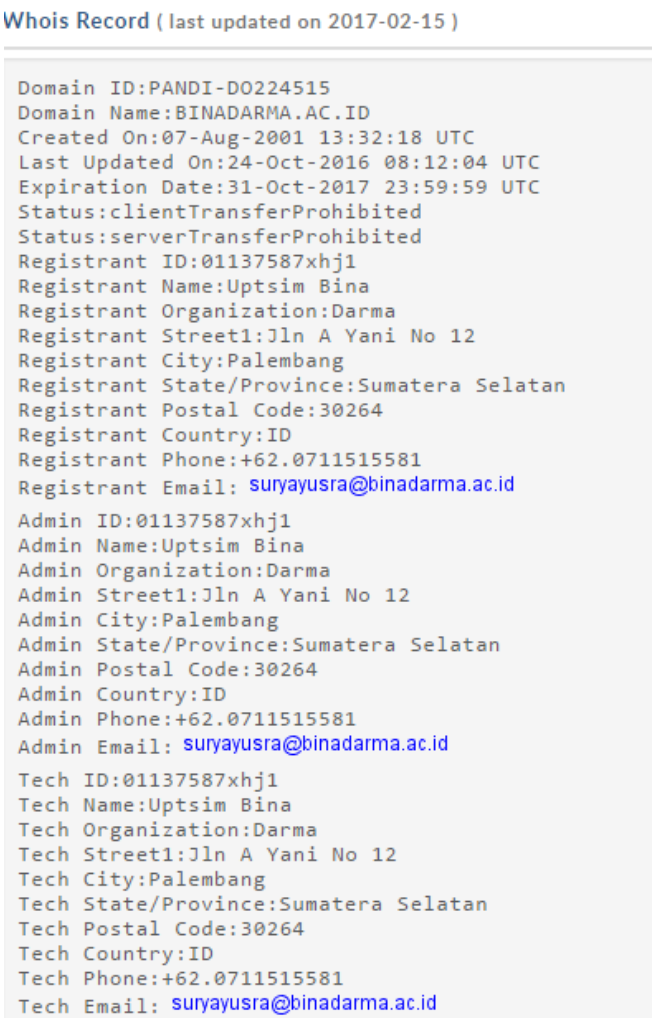
Website

Website Title	Portal Web UBD | Universitas Bina Darma, Palembang, Indonesia | Universitas Bina Darma
Server Type	Apache/2.4.17 (Win32) OpenSSL/1.0.2d PHP/5.6.14
Response Code	200
SEO Score	72%
Terms	1178 (Unique: 506, Linked: 567)
Images	30 (Alt tags missing: 7)
Links	244 (Internal: 205, Outbound: 11)

Whois Record (last updated on 2017-02-15)

```
Domain ID:PANDI-DO224515
Domain Name:BINADARMA.AC.ID
```

Gambar.3 Informasi yang Didapatkan dari Tools Whois (1)



Whois Record (last updated on 2017-02-15)

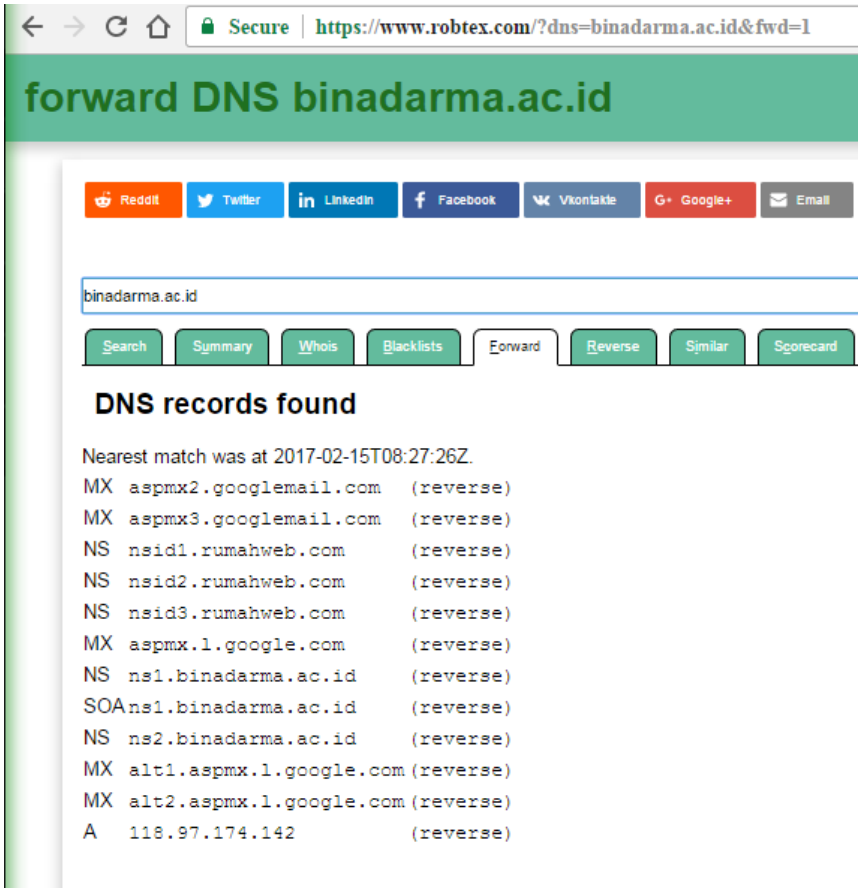
```
Domain ID:PANDI-DO224515
Domain Name:BINADARMA.AC.ID
Created On:07-Aug-2001 13:32:18 UTC
Last Updated On:24-Oct-2016 08:12:04 UTC
Expiration Date:31-Oct-2017 23:59:59 UTC
Status:clientTransferProhibited
Status:serverTransferProhibited
Registrant ID:01137587xhj1
Registrant Name:Uptsim Bina
Registrant Organization:Darma
Registrant Street1:Jln A Yani No 12
Registrant City:Palembang
Registrant State/Province:Sumatera Selatan
Registrant Postal Code:30264
Registrant Country:ID
Registrant Phone:+62.0711515581
Registrant Email: suryayusra@binadarma.ac.id

Admin ID:01137587xhj1
Admin Name:Uptsim Bina
Admin Organization:Darma
Admin Street1:Jln A Yani No 12
Admin City:Palembang
Admin State/Province:Sumatera Selatan
Admin Postal Code:30264
Admin Country:ID
Admin Phone:+62.0711515581
Admin Email: suryayusra@binadarma.ac.id

Tech ID:01137587xhj1
Tech Name:Uptsim Bina
Tech Organization:Darma
Tech Street1:Jln A Yani No 12
Tech City:Palembang
Tech State/Province:Sumatera Selatan
Tech Postal Code:30264
Tech Country:ID
Tech Phone:+62.0711515581
Tech Email: suryayusra@binadarma.ac.id
```

Gambar.4 Informasi yang Didapatkan dari Tools Whois (2)

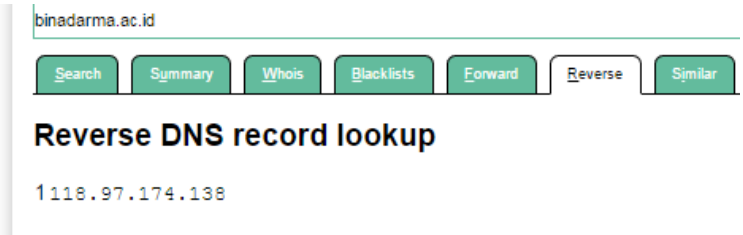
```
Billing ID:01137587xhj1
Billing Name:Uptsim Bina
Billing Organization:Darma
Billing Street1:Jln A Yani No 12
Billing City:Palembang
Billing State/Province:Sumatera Selatan
Billing Postal Code:30264
Billing Country:ID
Billing Phone:+62.0711515581
Billing Email: suryayusra@binadarma.ac.id

Sponsoring Registrar ID:digitalreg
Sponsoring Registrar Organization:Digital Registra
Sponsoring Registrar Postal Code:55281
Sponsoring Registrar Country:ID
Sponsoring Registrar Phone:0274882257
Name Server:NS1.BINADARMA.AC.ID
Name Server:NS2.BINADARMA.AC.ID
DNSSEC:Unsigned
```

Gambar.5 Informasi yang Didapatkan dari Tools Whois (3)

Dari hasil whois seperti Gambar.3 hingga Gambar.5 diatas, didapatkanlah informasi berupa : domain id, domain name, catatan tanggal dan waktu domain dibuat, catatan tanggal dan waktu domain diupdate, name server, registrant, admin, tech, billing dan sponsoring yang berisikan : id, nama, organisasi, alamat, kota, provinsi, kode pos, nomor telepon dan email.



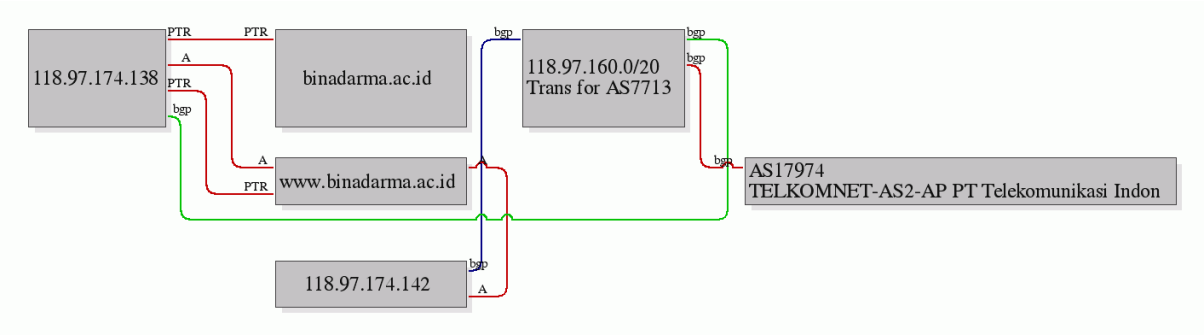
Gambar.6 DNS Record



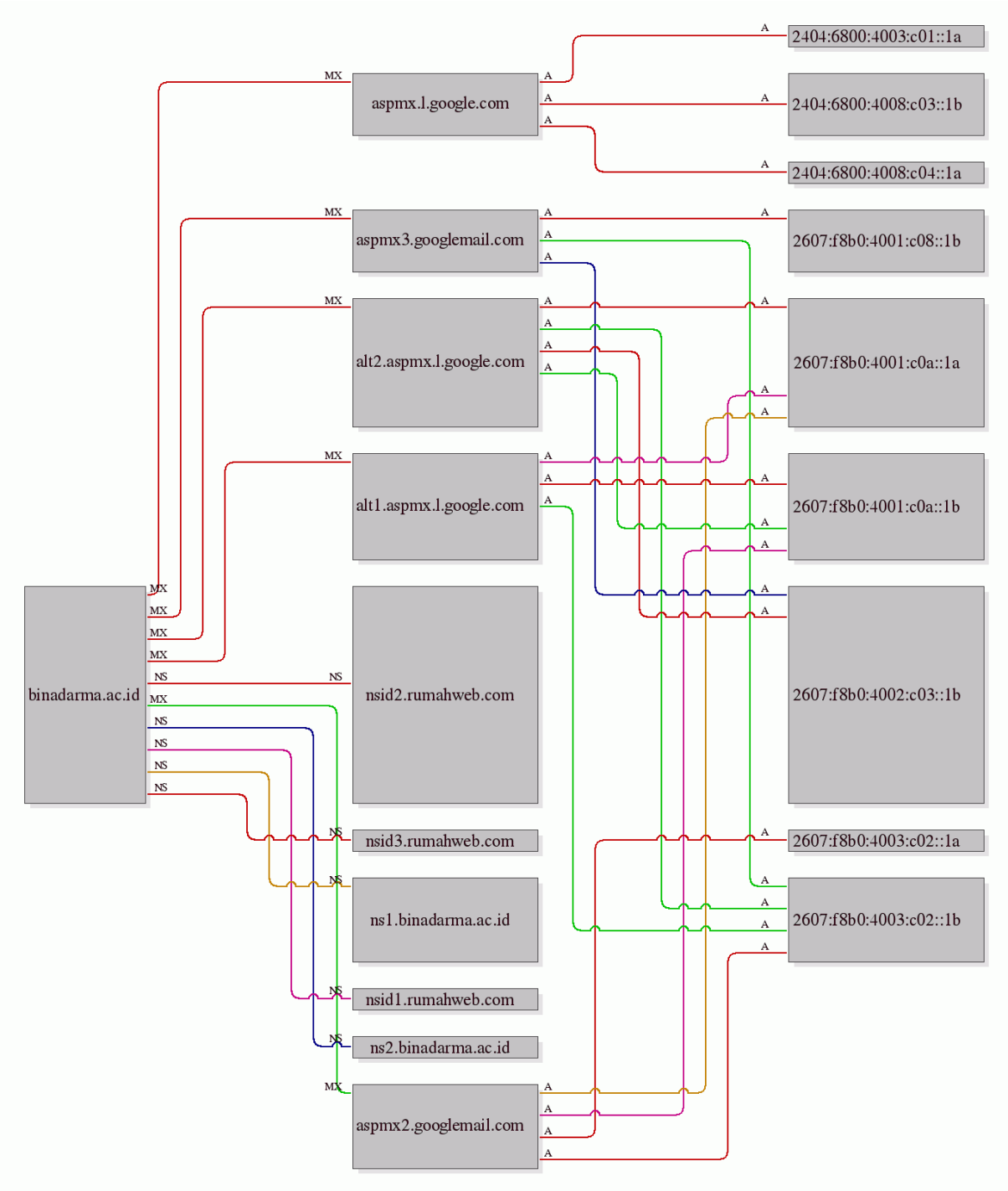
Gambar.7 Reverse DNS Record

Reverse yang telah dilakukan megarah ke dua alamat IP : 118.97.174.138 dan 118.97.174.142 dalam naungan AS7713 di Indonesia seperti grafik dibawah ini.

Nama : Leny Novita Sari
NIM : 09011181320027
Keamanan Jaringan Komputer



Gambar.8 Grafik Reverse DNS Record



Gambar.8 Grafik Domain binadarma.ac.id

Dari domain binadarma.ac.id terdapat lima name server yang tidak menggunakan nama domain, yaitu : nsid1.rumahweb.com, nsid2.rumahweb.com, nsid3.rumahweb.com, ns1.binadarma.ac.id dan ns2.binadarma.ac.id.

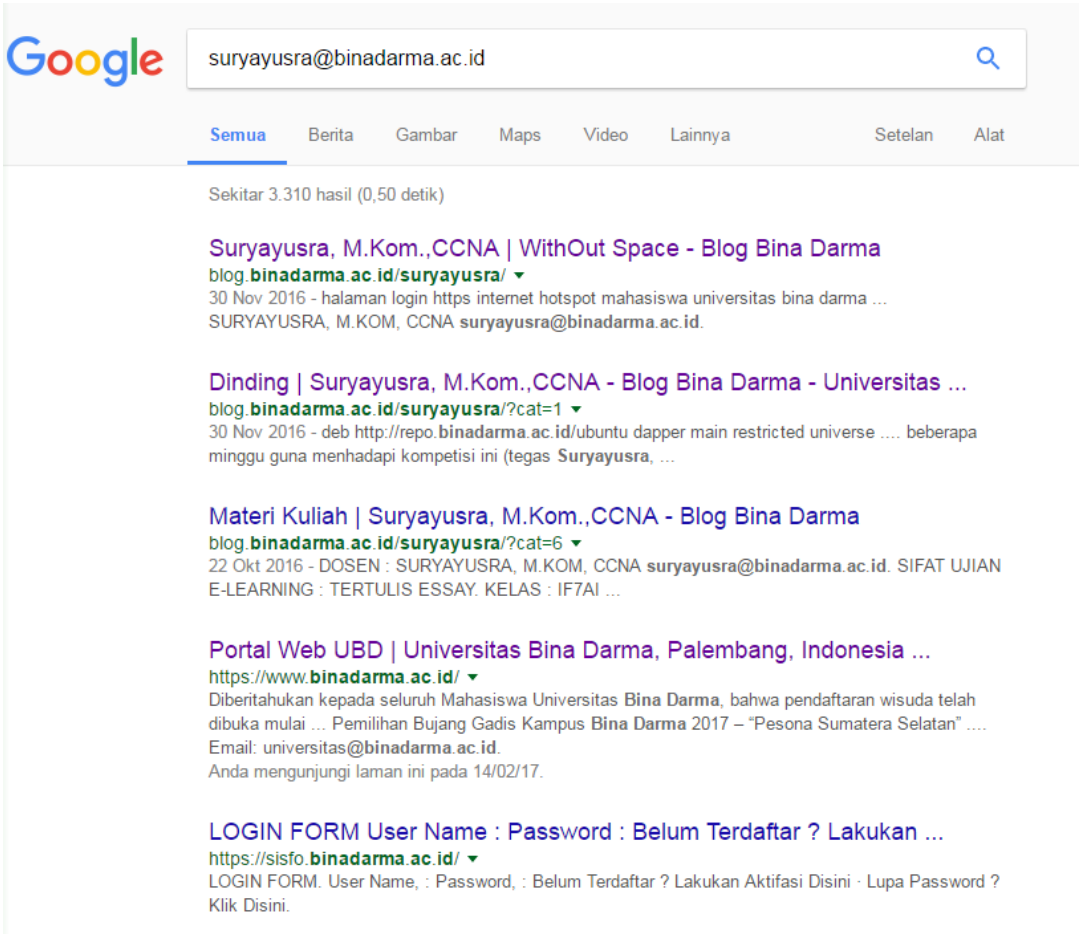
Lima mail server yang tidak menggunakan nama domain, yaitu : aspmx2.googlemail .com, aspmx3.googlemail.com, aspmx.l.google.com, alt1.aspmx.l.google.com dan alt2.aspmx .l.google.com selanjutnya disebut sebagai kelompok mail server-1.

Ada beberapa ratus domain yang menggunakan name server nsid3.rumahweb.com, tiga perempat dari mereka menggunakan tujuh name server : nsid3.rumahweb.biz, nsid1.rumahweb.com, nsid2.rumahweb.com, nsid3.rumahweb.com, nsid4.rumahweb.com, nsid2.rumahweb.net dan nsid4.rumahweb.org. Sepertiga dari mereka mengarah pada empat alamat IP 216.239.32.21, 216.239.34.21, 216.239.36.21 dan 216.239.38.21 yang dinaungi oleh Google in Mountain View, United States. Enam persen dari mereka menggunakan kelompok mail server-1 dan dua belas dari mereka mengarah ke dua alamat IP, yaitu : 202.69.110.87 dan 103.247.10.131.

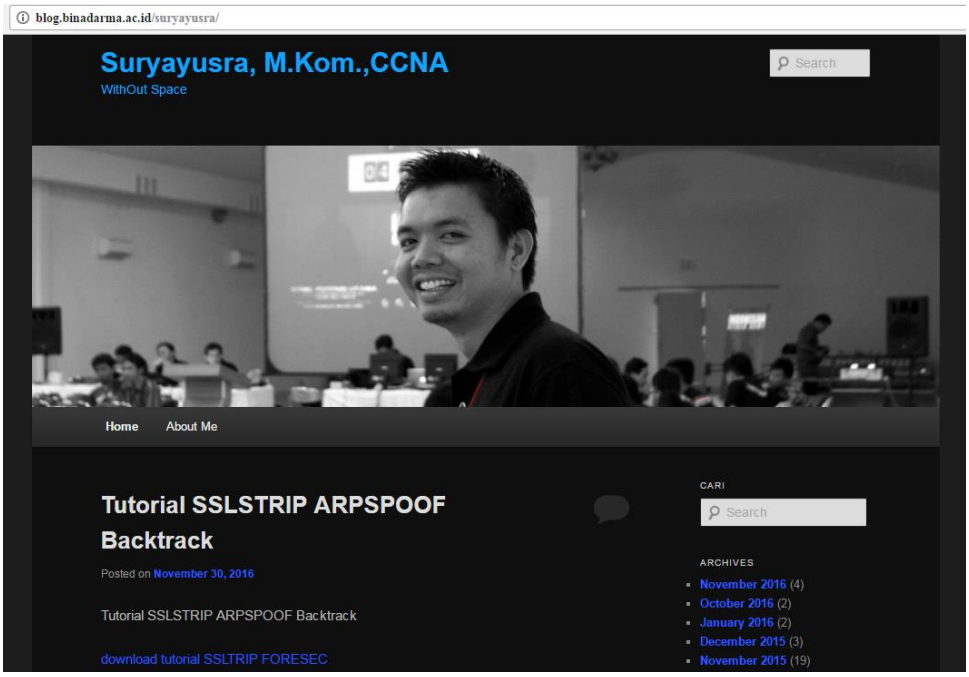
Sistem operasi, subdomain terkait dan kapan terakhir diupdate dari target dapat kita ketahui dengan tools netcraft. Semakin old OS yang digunakan maka semakin rentan keamanannya.

Gambar.9 Netcraft

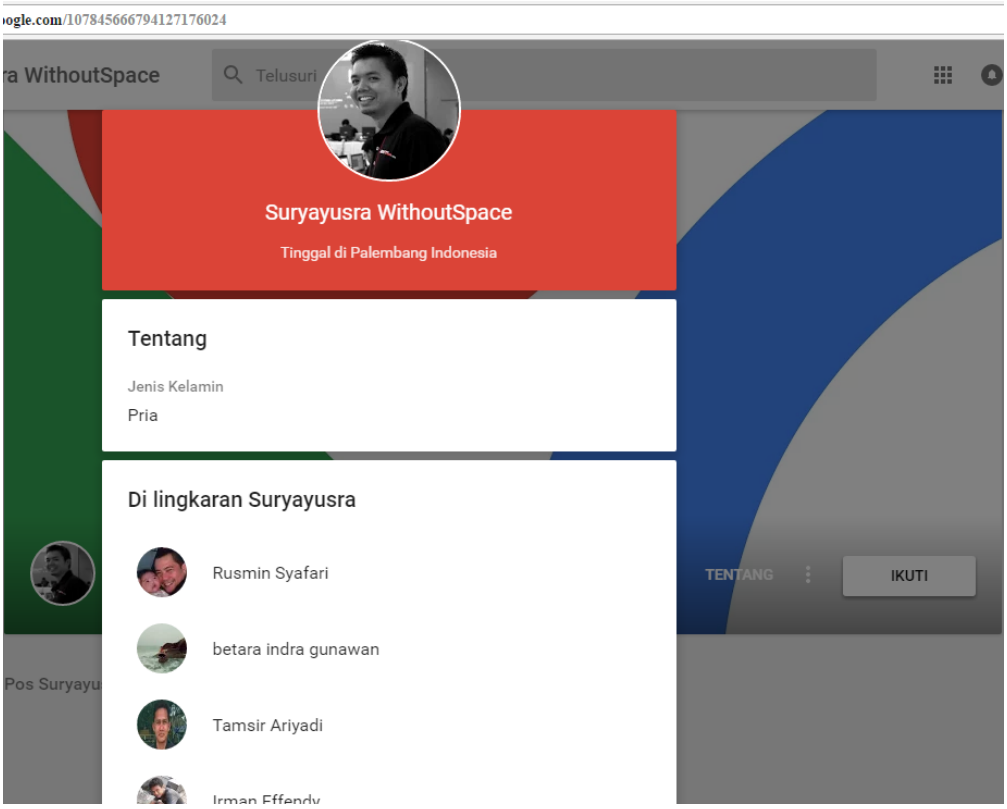
Dengan informasi yang didapatkan dari whois diatas juga, kita dapat menggali informasi lebih jauh lagi seperti rekayasa sosial untuk mengkonsolidasikan sejumlah besar data yang dapat digunakan untuk melakukan pengintaian dari lingkungan target seperti dibawah ini.



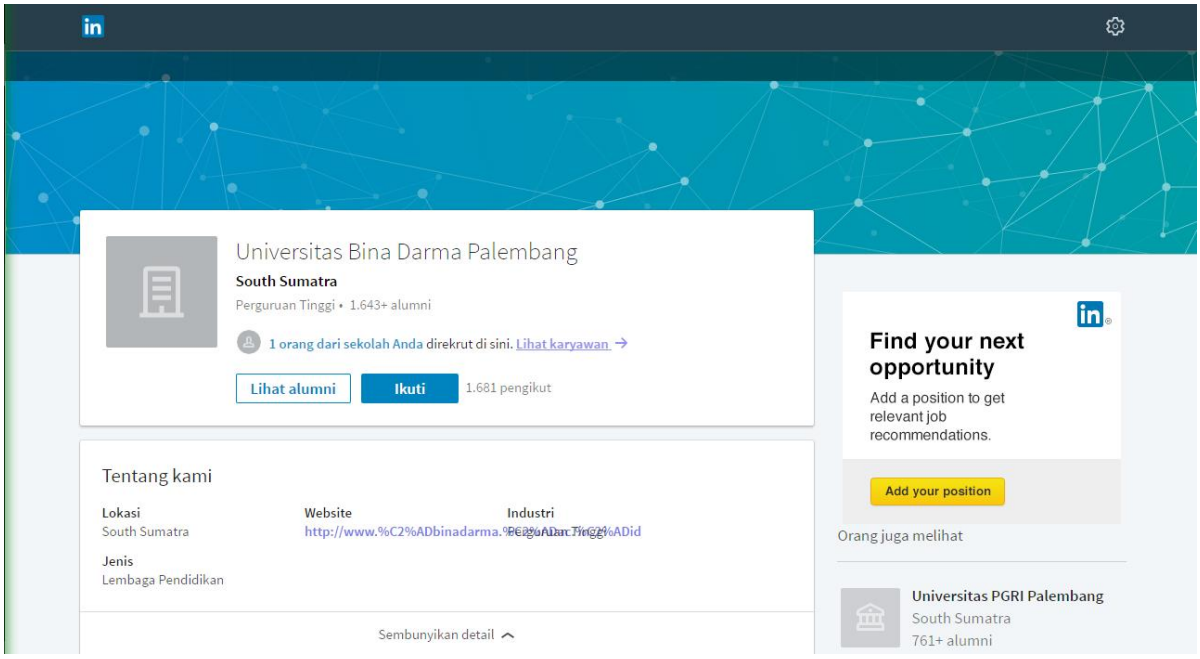
Gambar.10 Rekayasa sosial (1)



Gambar.11 Rekayasa sosial (2)



Gambar.12 Rekayasa sosial (3)



Gambar.13 Rekayasa sosial dengan Mencari Target pada "Lihat Karyawan" pada Linkedin UBDP