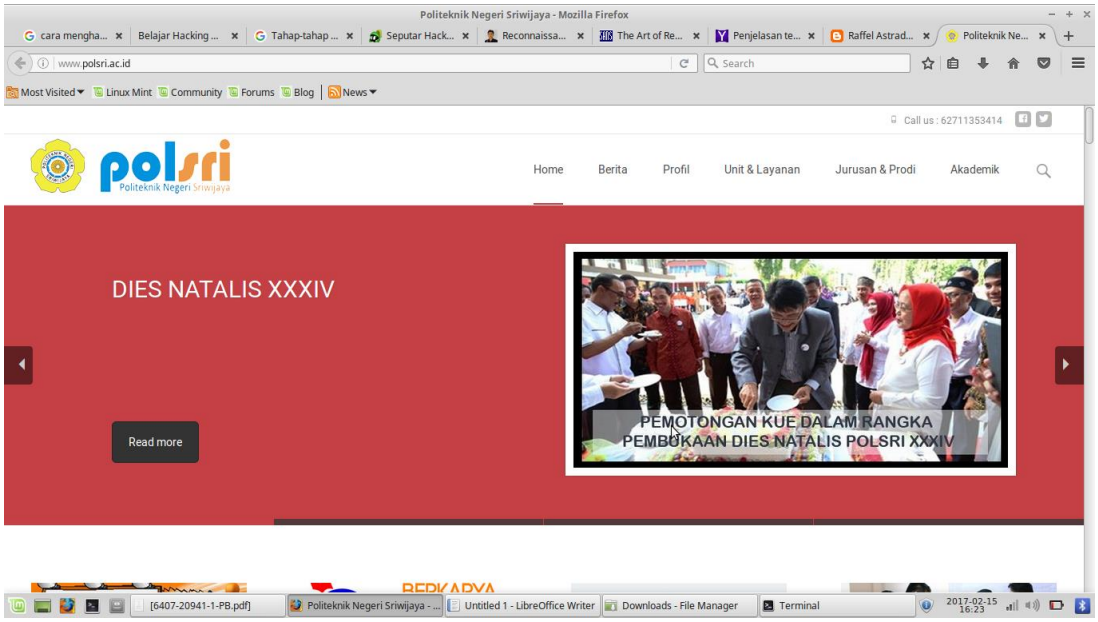
Nama : Riki Andika
NIM : 09011181320015

Reconnaissance ialah tahapan seorang Hacker dalam mengumpulkan data sebanyak banyaknya tentang target atau sasaran yang akan diserang atau dibobol websitenya, dengan menggali informasi berupa tanggal lahir, nomor rumah, nama istri atau suami atau anak, hobi, plat kendaraan, dll. Reconnaissance dibagi menjadi 2, yaitu Active Reconnaissance dan Passive Reconnaissance. Active Reconnaissance adalah pengumpulan data dengan cara bertatap muka langsung atau berhubungan langsung dengan Target/Sasaran, sedangkan Passive Reconnaissance adalah menggunakan media informasi seperti berita, internet, dan lain-lain.

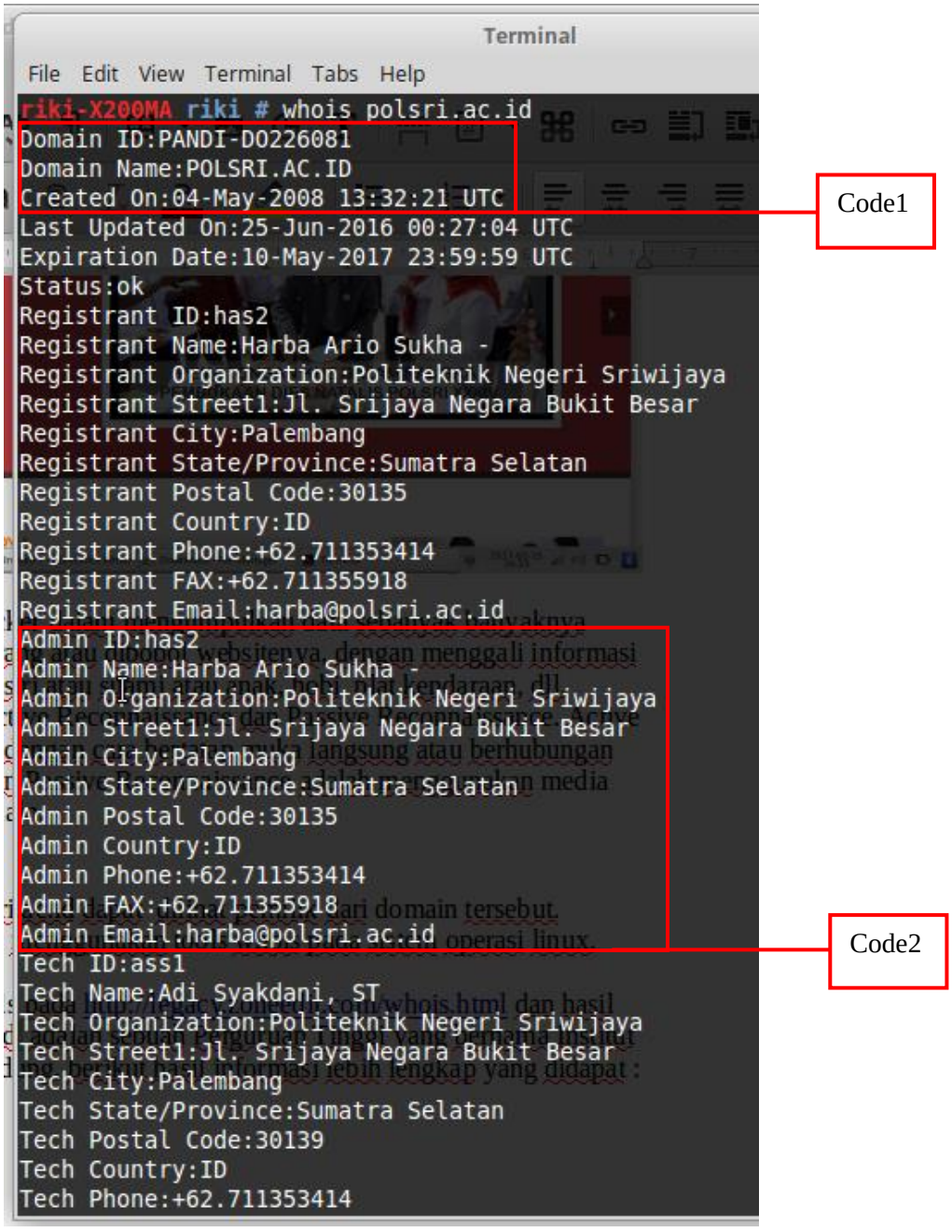
Website sasaran yang akan direconnaissance ialah website Politeknik Negeri Sriwijaya Palembang dengan alamat dimain www.polsri.ac.id, berikut screenshoot tampilan dari website Politeknik Negeri Sriwijaya Palembang.



Gambar 1. Tampilan website Politeknik Negeri Sriwijaya Palembang

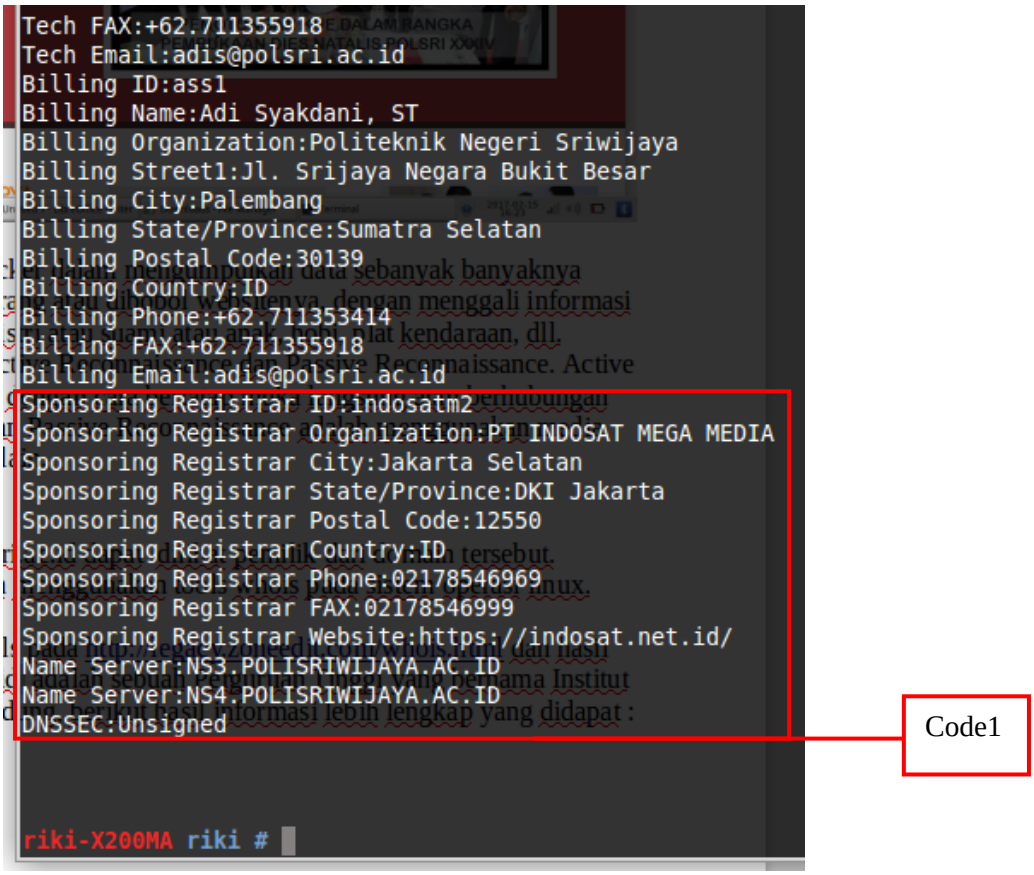
Hasil yang didapat dari domain www.polsri.ac.id dapat dilihat pemilik dari domain tersebut. Berikut hasil capture yang didapat, dengan menggunakan tools whois yang dijalankan pada sistem operasi linux. Untuk domain www.polsri.ac.id menggunakan

tools whois yang dijalankan pada sistem operasi linux dan hasil yang didapat untuk pemilik domain www.polsri.ic.id adalah sebuah Perguruan Tinggi Negeri yang bernama Politeknik Negeri Sriwijaya yang berlokasi dikota Palembang, Provinsi Sumatera Selatan, berikut hasil informasi lebih lengkap yang didapat, pada **Gambar 2** dan **Gambar 3.**



Gambar 2. Informasi lengkap dengan menggunakan tools whois

Pada **Gambar 2** memberikan informasi yang berkaitan dengan domain yang dijadikan target, dengan informasi-informasi yang dapat dijadikan sebagai acuan. Pada code1 yang ada pada **Gambar 2**, memberikan informasi berupa ID Domain dan Nama Domain yang digunakan, dengan ID Domain PANDI-D0226081 dan dengan Nama Domain POLSRI.AC.ID. Informasi mendasar seperti ini dapat dijadikan acuan untuk melakukan sebuah pengintaian pada suatu website. Pada code 2 yang ada pada **Gambar 2**, memberikan informasi mengenai admin yang menjalakan atau mengoperasikan website tersebut, seperti informasi nama, alamat, nomor telephone, email serta informasi lain yang berhubungan dengan admin.



Gambar 3. Informasi lengkap dengan menggunakan tools whois

Banyaknya data yang didapat dalam melakukan sebuah pengintai suatu website ini dapat memberi kemudahan kepada pengitai untuk menemukan tujuan utama dari proses pengintaian yang dilakukan. Pada code 1 yang ada pada gambar 3, memberikan informasi mengenai sponsor yang menjalin hubungan demi kelancaran penggunaan

website tersebut, dapat dilihat pada gambar 3 informasi sponsor yang diperoleh cokup lengkap, seperti ID, nama organisasi, alamat lengkap, serta website dari penyedia atau sponsor tersebut, dan juga informasi mengenai DNS Server yang digunakan (ns3.polsri.ac.id dan ns4.polsri.ac.id) . Berikut traceroute atau loncatan hops yang dilalui untuk sampai ke domain sasaran, dapat dilihat pada **Gambar 4.**

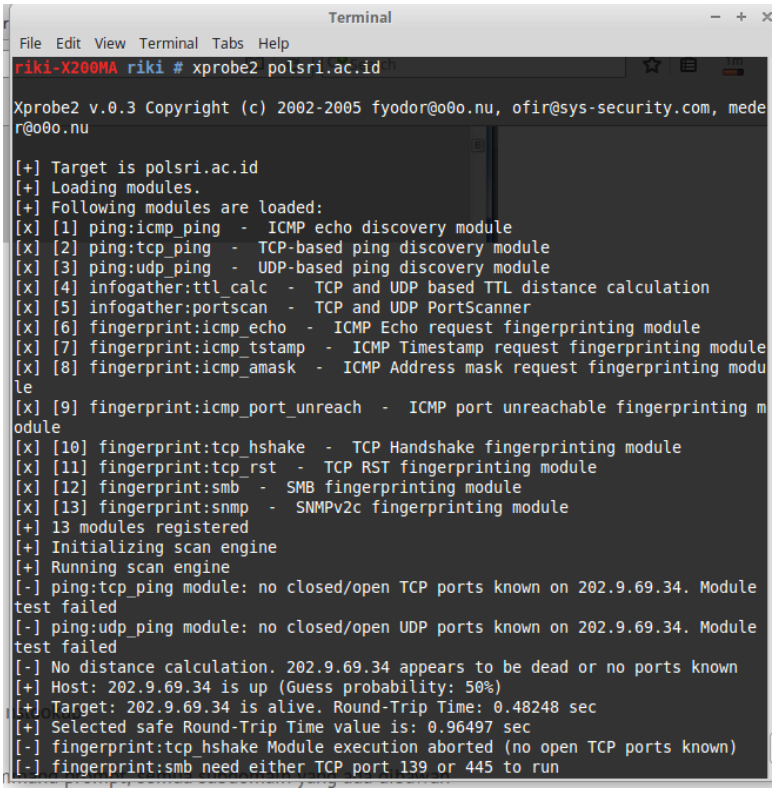
TraceRoute from Network-Tools.com to 202.9.69.34 [polsri.ac.id]

Hop	(ms)	(ms)	(ms)	IP Address	Host name
1	0	0	0	206.123.64.153	-
2	3	0	0	206.123.64.158	-
3	1	1	1	129.250.202.253	xe-0-4-0-12.r01.dllstx04.us.bb.gin.ntt.net
4	1	1	1	129.250.6.128	ae-2.r23.dllstx09.us.bb.gin.ntt.net
5	39	39	39	129.250.4.154	ae-8.r23.snjsca04.us.bb.gin.ntt.net
6	39	39	39	129.250.2.182	ae-0.r22.snjsca04.us.bb.gin.ntt.net
7	202	202	202	129.250.3.49	ae-2.r20.sngpsi05.sg.bb.gin.ntt.net
8	203	202	203	129.250.7.19	ae-1.r00.sngpsi05.sg.bb.gin.ntt.net
9	207	208	207	116.51.26.130	-
10	226	226	226	202.9.69.34	www.polsri.ac.id

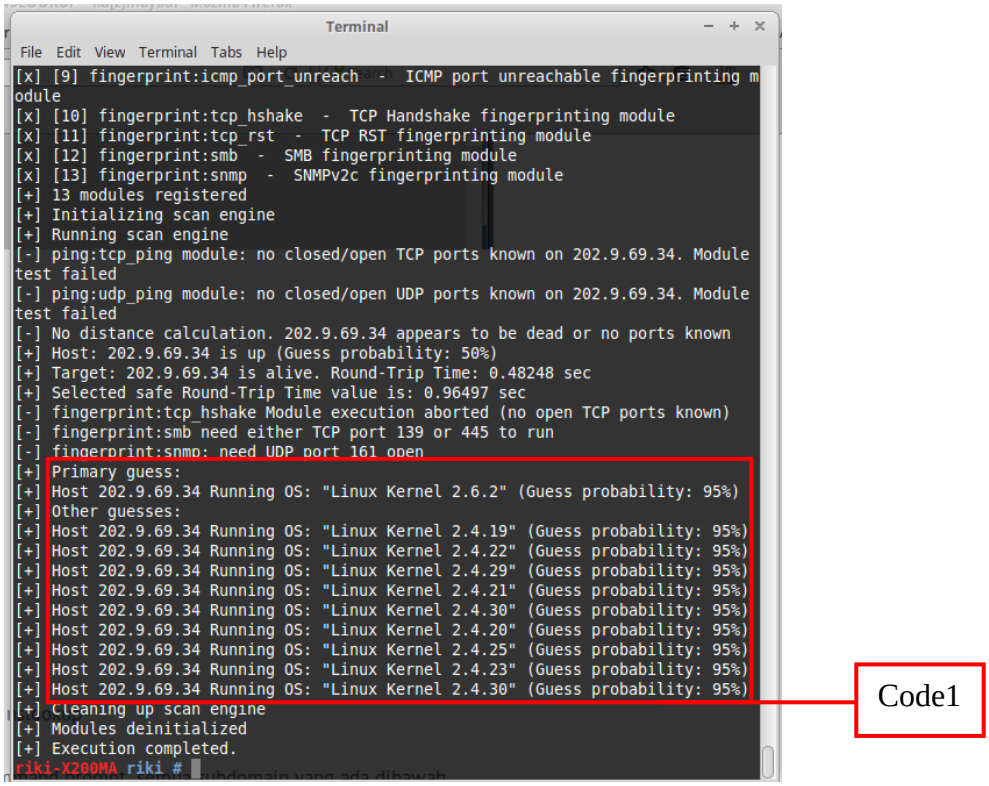
Trace complete

Gambar 4. Traceroute untuk sampai pada domain sasaran

Gambar 4 menjelaskan proses yang dilewati sebuah paket untuk mencapai tujuannya dengan mengirimkan pesan Internet Control Message Protocol (ICMP) Echo Request ke tujuan berdasarkan alamat IP tujuan dengan nilai Time to Live yang semakin meningkat. Pada kasus ini banyaknya loncatan yang dilakukan untuk sampai kealamat tujuan sebanyak 10 hops yang diloncati atau dilalui. Mengenai penggunaan IP Address pada website sasaran dapat dilihat pada **Gambar 5**, dengan menggunakan tools xprobe2 yang dijalankan pada sistem operasi linux.



Gambar 5. Penggunaan tools xprobe2



Gambar 6. Penggunaan tools xprobe2 (lanjutan)

IP Adress merupakan deretan bilangan biner di antara 32 bit hingga 128 bit yang dipakai sebagai media untuk mengidentifikasi untuk setiap perangkat komputer yang terhubung pada jaringan komputer (intranet / internet). Pada kasus ini website sasaran menggunakan IP Versi 4 yang termasuk dalam kelas C, dengan IP Address 202.9.69.34, dan Sistem Operasi yang digunakan ialah Linux Kernel Versi 2.6.2. Penggunaan linux kernel Versi 2.6.2 dapat membuat beberapa buffer overflows dalam fungsi cmtp_recv_interopmsg pada driver Bluetooth (net / bluetooth / cmtp / capi.c) di kernel Linux 2.4.22 sampai dengan 2.4.33.4 dan 2.6.2 sebelum 2.6.18.6, dan 2.6.19.x, memungkinkan penyerang remote untuk menyebabkan penolakan layanan (crash) dan mungkin mengeksekusi kode arbitrary melalui pesan CAPI dengan nilai besar untuk panjang manu (produsen) atau serial (serial number) bidang.