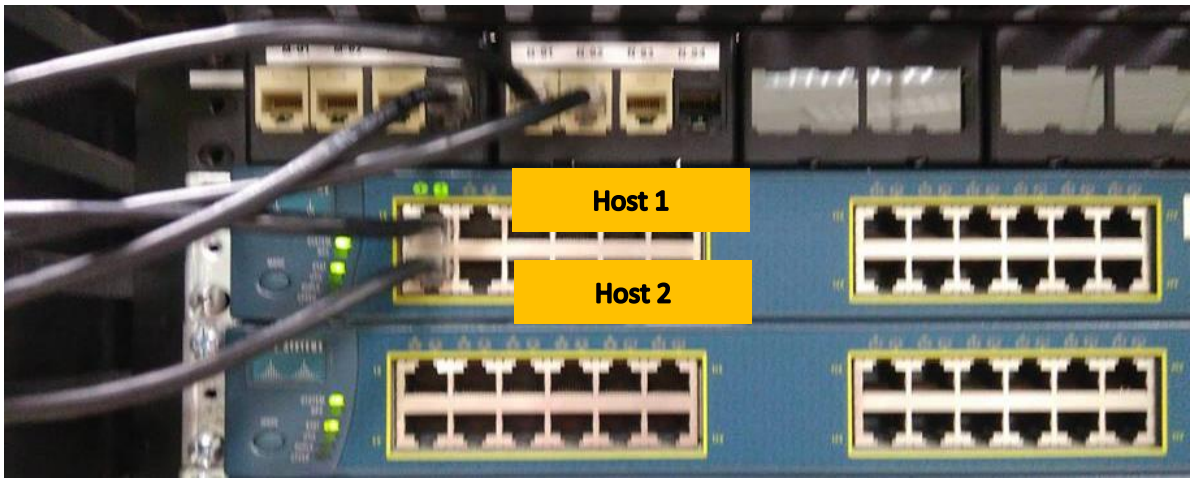
Instituto Tecnológico y de Estudios Superiores de Monterrey

Jonathan Torres Escárcega A00759281
Seguridad Informática Avanzada 28/08/2017

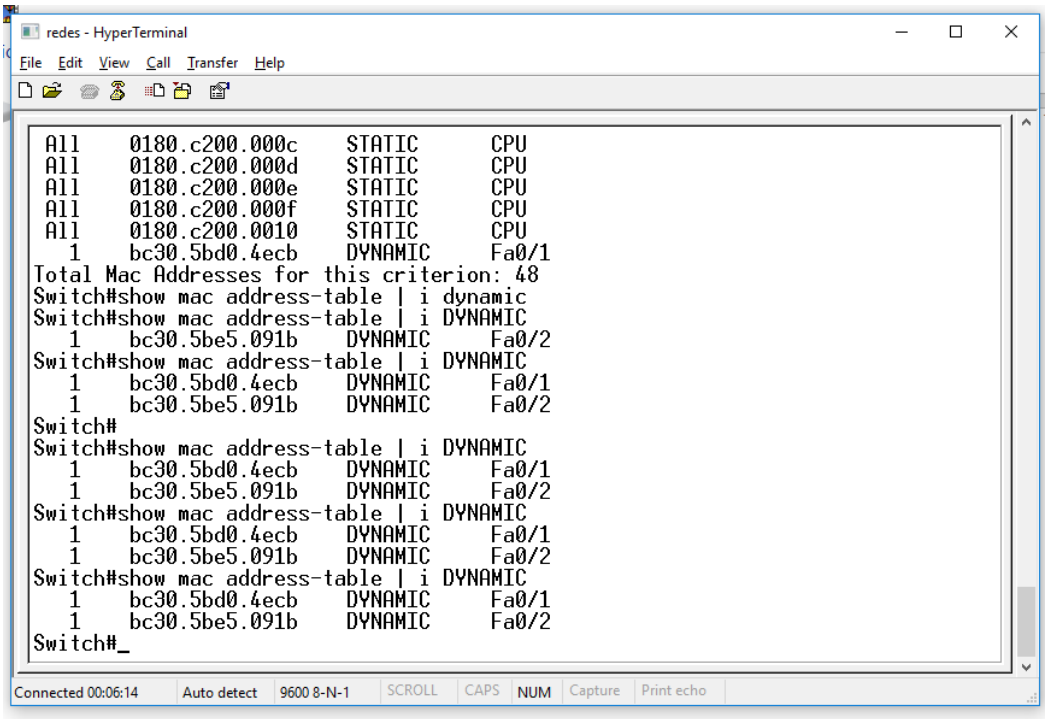
Práctica de Laboratorio #2

1. Foto de la topología armada:

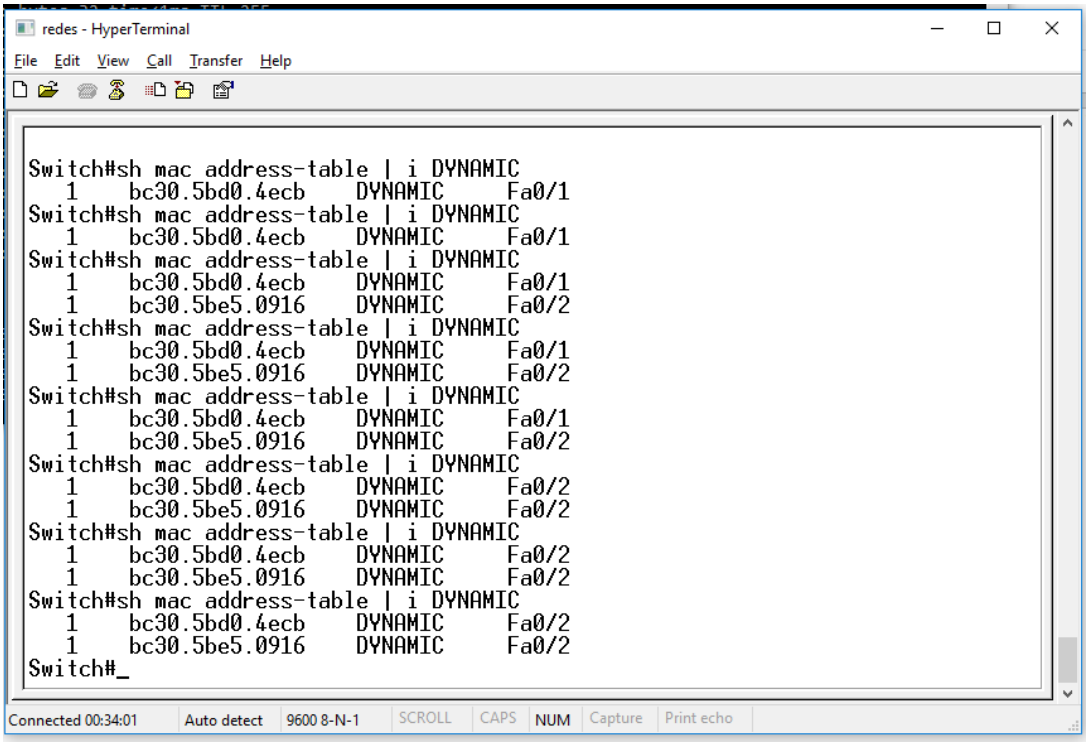


2. Mac address table antes y después del ataque:

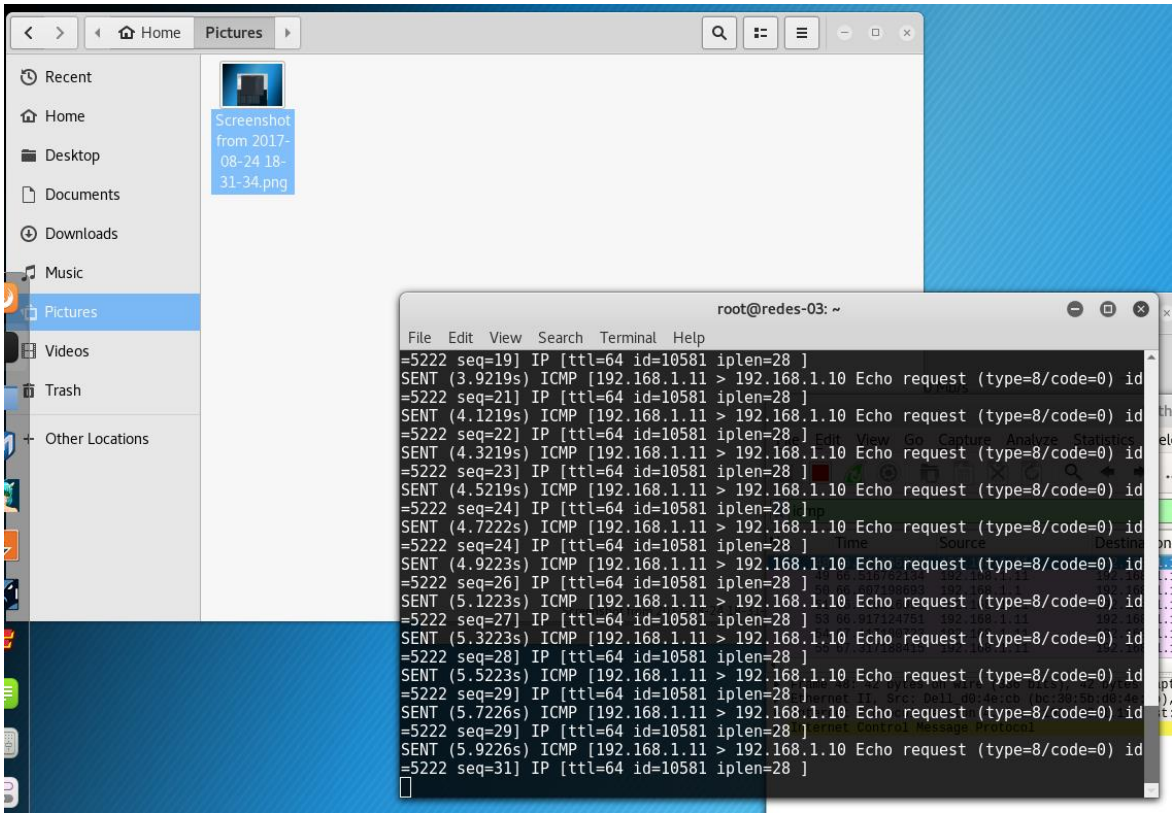
Antes:



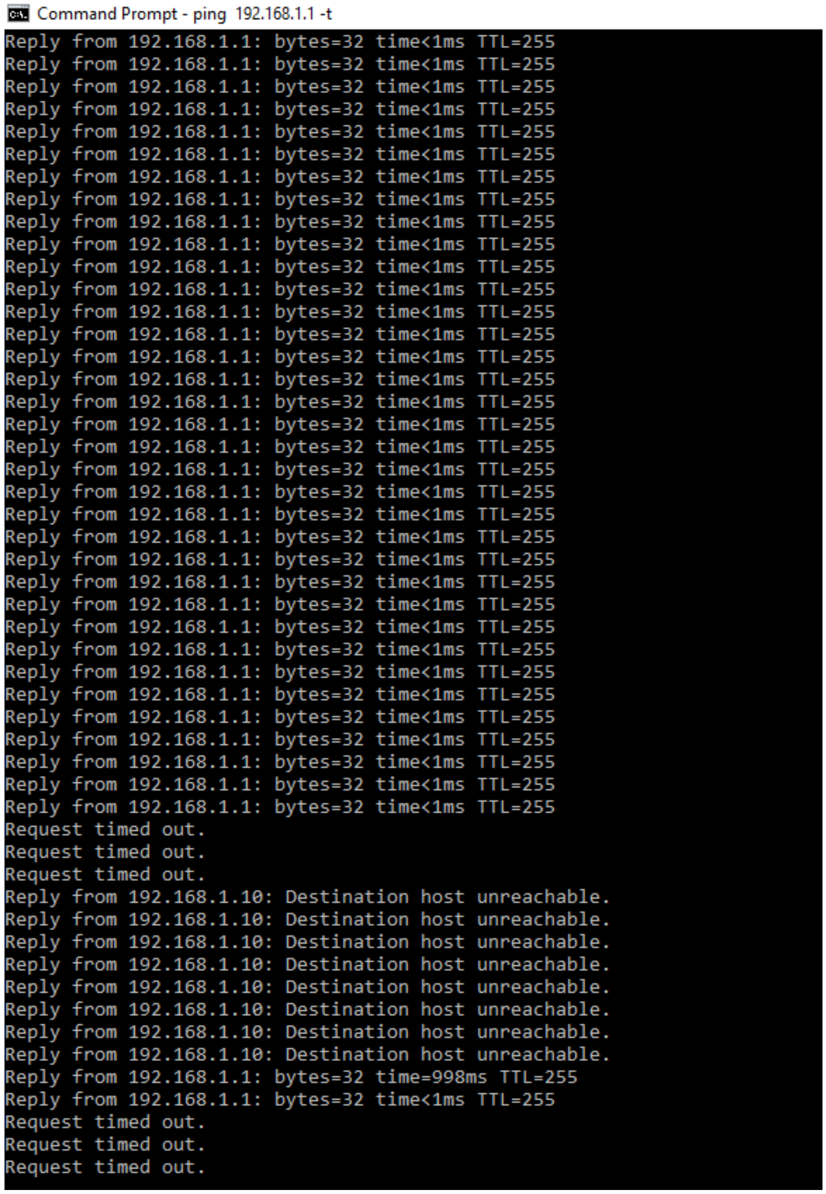
Después:



3. Ataque desde Kali Linux:

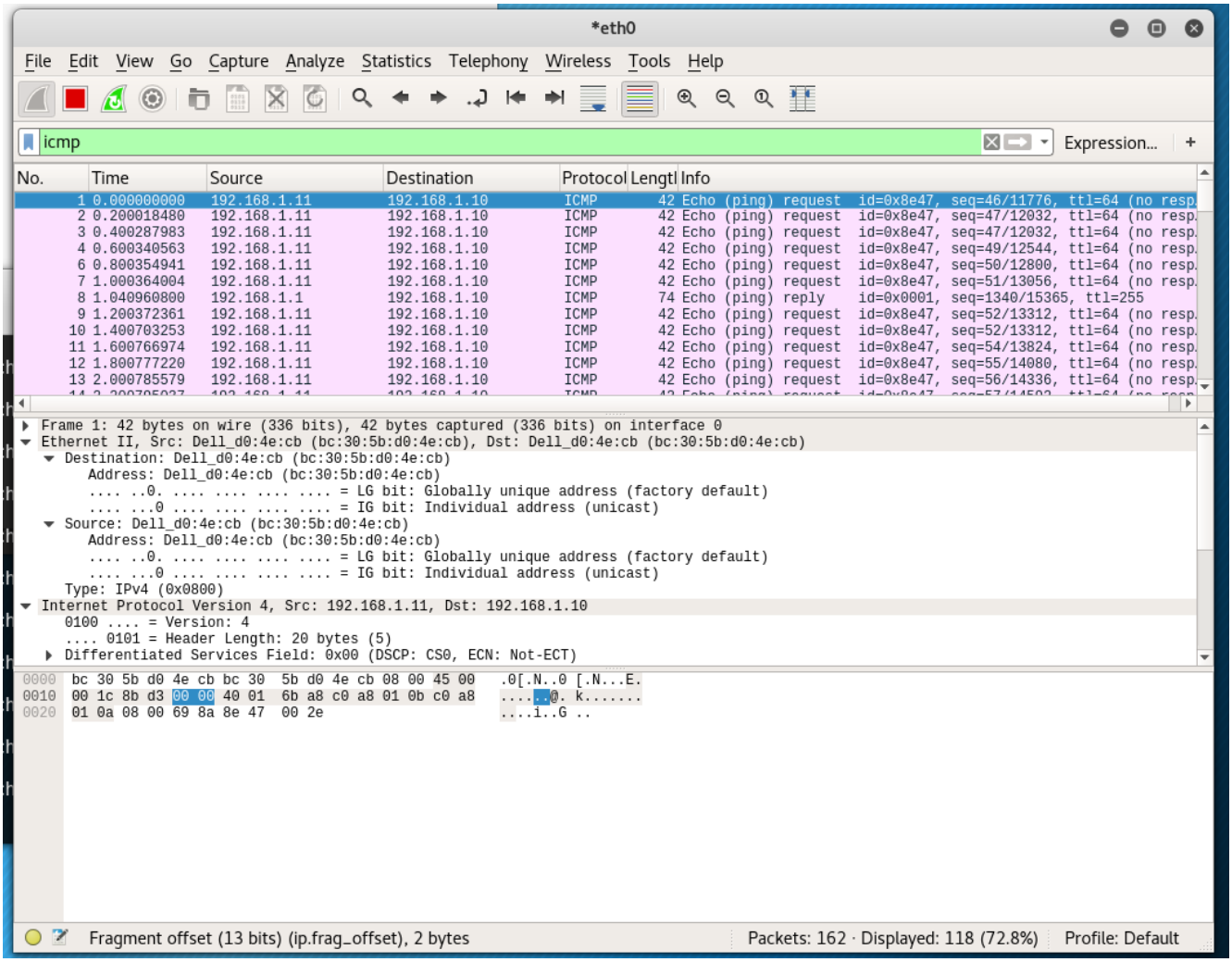


4. Host 1 pierde conectividad:



```
Command Prompt - ping 192.168.1.1 -t
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Request timed out.
Request timed out.
Request timed out.
Reply from 192.168.1.10: Destination host unreachable.
Reply from 192.168.1.10: Destination host unreachable.
Reply from 192.168.1.10: Destination host unreachable.
Reply from 192.168.1.10: Destination host unreachable.
Reply from 192.168.1.10: Destination host unreachable.
Reply from 192.168.1.10: Destination host unreachable.
Reply from 192.168.1.10: Destination host unreachable.
Reply from 192.168.1.10: Destination host unreachable.
Reply from 192.168.1.1: bytes=32 time=998ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Request timed out.
Request timed out.
Request timed out.
```

5. Monitoreo desde WireShark:


*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
icmp
Expression...
No. Time Source Destination Protocol Lengt Info
1 0.000000000 192.168.1.11 192.168.1.10 ICMP 42 Echo (ping) request id=0x8e47, seq=46/11776, ttl=64 (no resp
2 0.200018480 192.168.1.11 192.168.1.10 ICMP 42 Echo (ping) request id=0x8e47, seq=47/12032, ttl=64 (no resp
3 0.400287983 192.168.1.11 192.168.1.10 ICMP 42 Echo (ping) request id=0x8e47, seq=47/12032, ttl=64 (no resp
4 0.600340563 192.168.1.11 192.168.1.10 ICMP 42 Echo (ping) request id=0x8e47, seq=49/12544, ttl=64 (no resp
6 0.800354941 192.168.1.11 192.168.1.10 ICMP 42 Echo (ping) request id=0x8e47, seq=50/12800, ttl=64 (no resp
7 1.000364004 192.168.1.11 192.168.1.10 ICMP 42 Echo (ping) request id=0x8e47, seq=51/13056, ttl=64 (no resp
8 1.040960800 192.168.1.1 192.168.1.10 ICMP 74 Echo (ping) reply id=0x0001, seq=1340/15365, ttl=255
9 1.200372361 192.168.1.11 192.168.1.10 ICMP 42 Echo (ping) request id=0x8e47, seq=52/13312, ttl=64 (no resp
10 1.400703253 192.168.1.11 192.168.1.10 ICMP 42 Echo (ping) request id=0x8e47, seq=52/13312, ttl=64 (no resp
11 1.600766974 192.168.1.11 192.168.1.10 ICMP 42 Echo (ping) request id=0x8e47, seq=54/13824, ttl=64 (no resp
12 1.800777220 192.168.1.11 192.168.1.10 ICMP 42 Echo (ping) request id=0x8e47, seq=55/14080, ttl=64 (no resp
13 2.000785579 192.168.1.11 192.168.1.10 ICMP 42 Echo (ping) request id=0x8e47, seq=56/14336, ttl=64 (no resp
Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0
Ethernet II, Src: Dell_d0:4e:cb (bc:30:5b:d0:4e:cb), Dst: Dell_d0:4e:cb (bc:30:5b:d0:4e:cb)
Destination: Dell_d0:4e:cb (bc:30:5b:d0:4e:cb)
Address: Dell_d0:4e:cb (bc:30:5b:d0:4e:cb)
.... ..0. .... = LG bit: Globally unique address (factory default)
....0 .... = IG bit: Individual address (unicast)
Source: Dell_d0:4e:cb (bc:30:5b:d0:4e:cb)
Address: Dell_d0:4e:cb (bc:30:5b:d0:4e:cb)
.... ..0. .... = LG bit: Globally unique address (factory default)
....0 .... = IG bit: Individual address (unicast)
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 192.168.1.11, Dst: 192.168.1.10
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
0000 bc 30 5b d0 4e cb bc 30 5b d0 4e cb 08 00 45 00 .0[.N..0 [.N...E.
0010 00 1c 8b d3 00 00 40 01 6b a8 c0 a8 01 0b c0 a8 ....@. k.....
0020 01 0a 08 00 69 8a 8e 47 00 2e ....i..G ..
Fragment offset (13 bits) (ip.frag_offset), 2 bytes
Packets: 162 · Displayed: 118 (72.8%)
Profile: Default