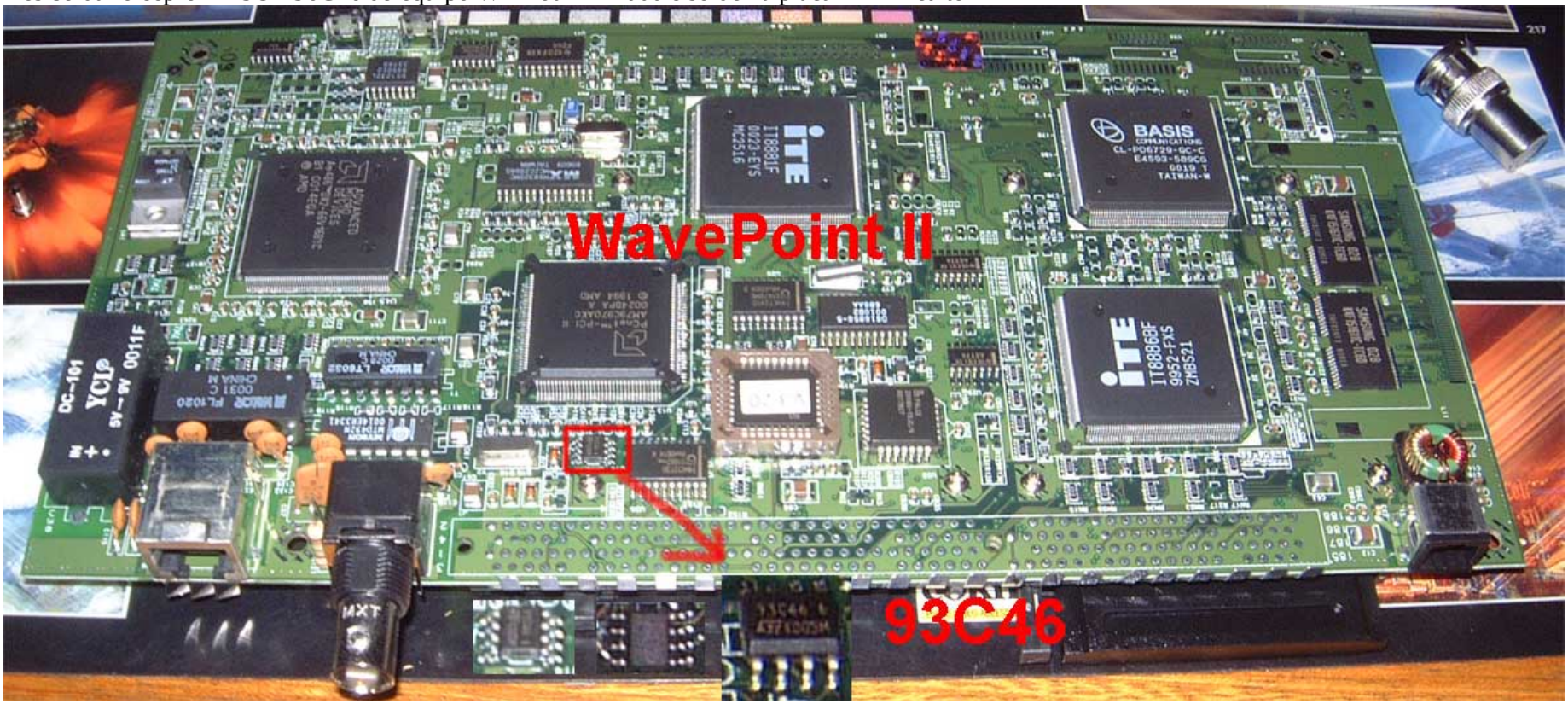
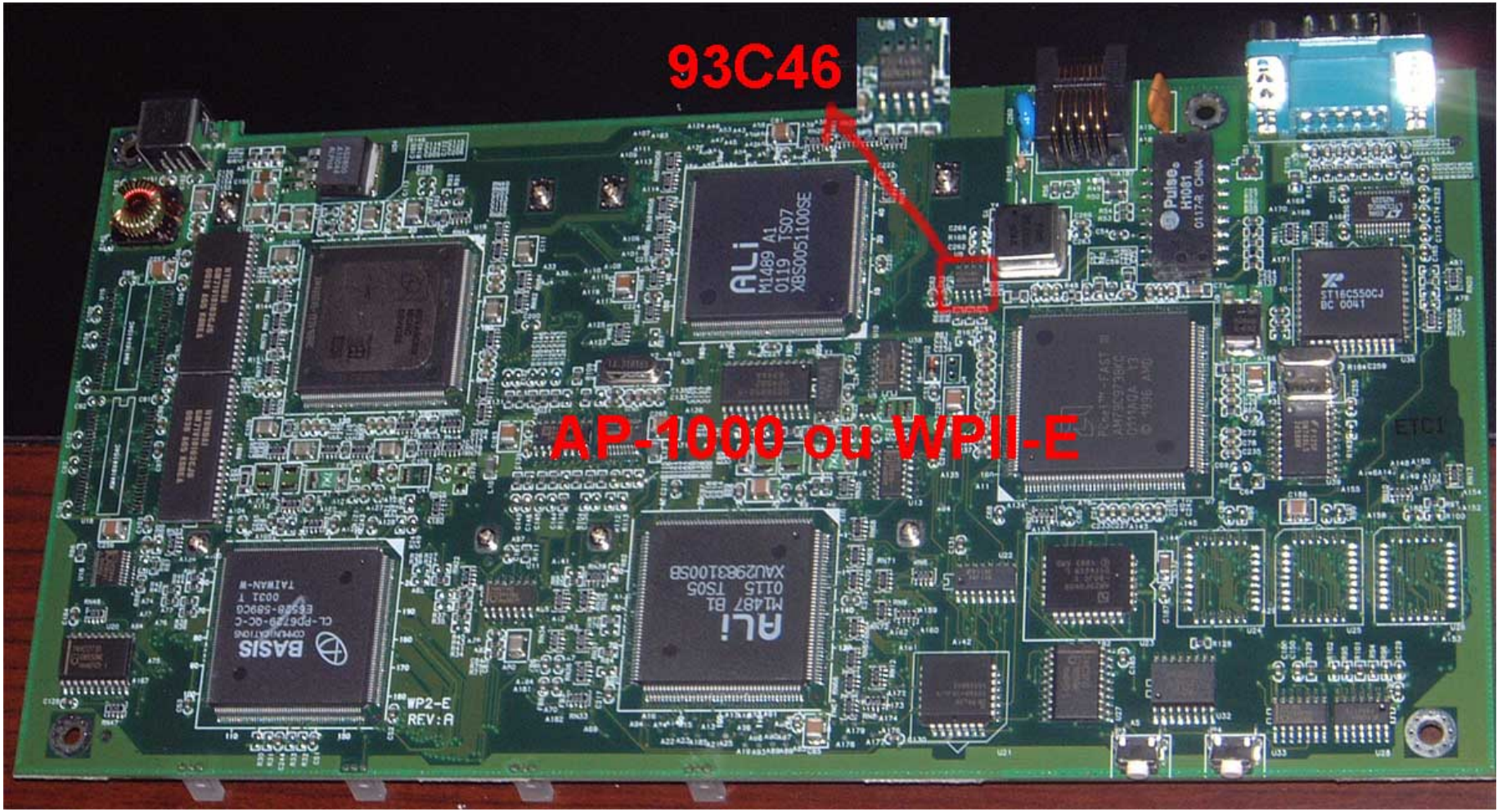
Para Hackeiar COR e ROR trocando MAC address dos WPII ou AP-1000

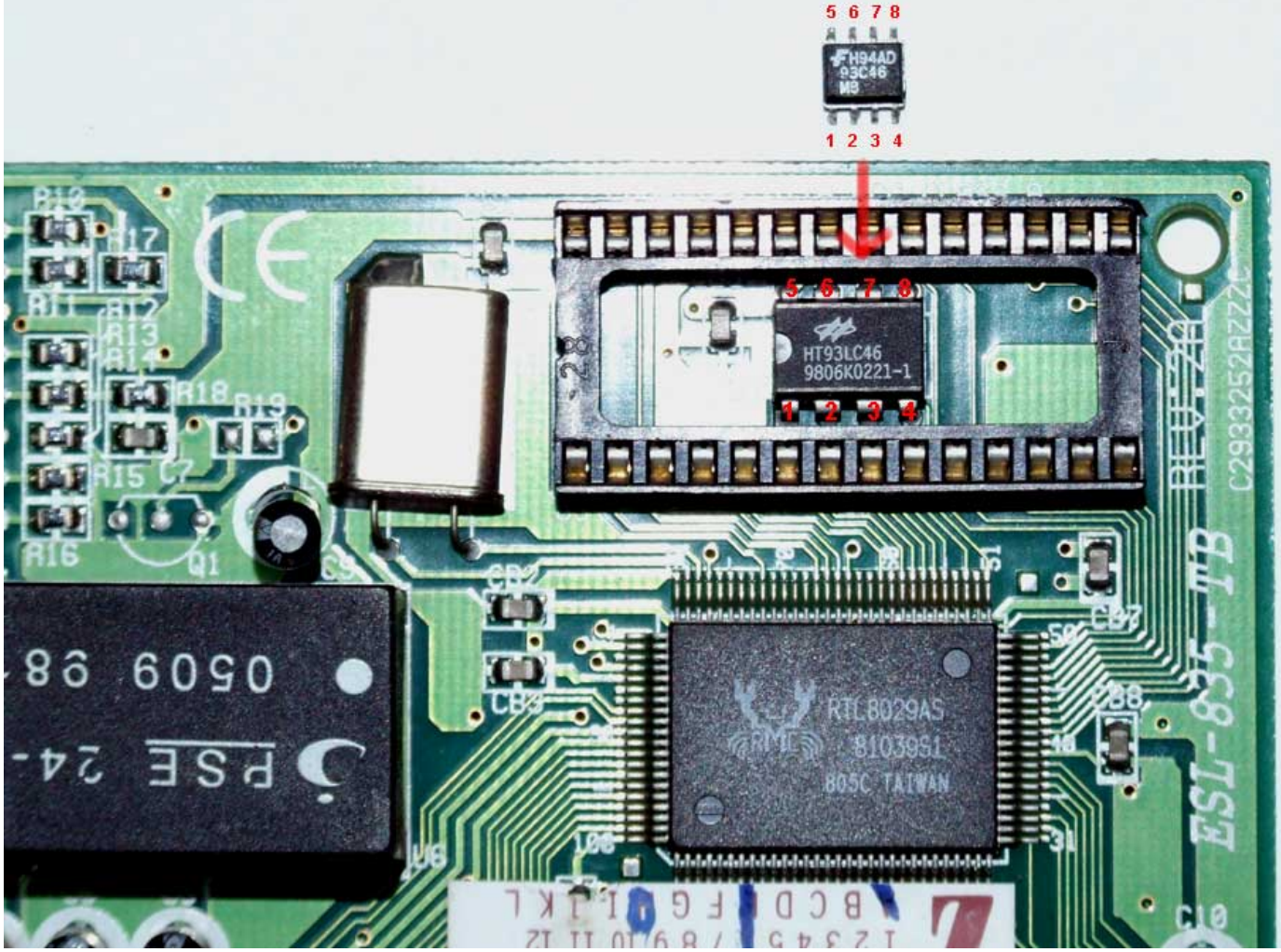
Arrumar uma placa LAN realtek com chipset rlt8029 e des-soldar o eeprom 96C46, solde os fios.

Dês-soldar o eeprom TSOP 96C46 do equipo WPII ou AP-1000 e solde na placa LAN Realtek




93C46
AP-1000 ou WPII-E

o Pino 6 nao é necessario soldar



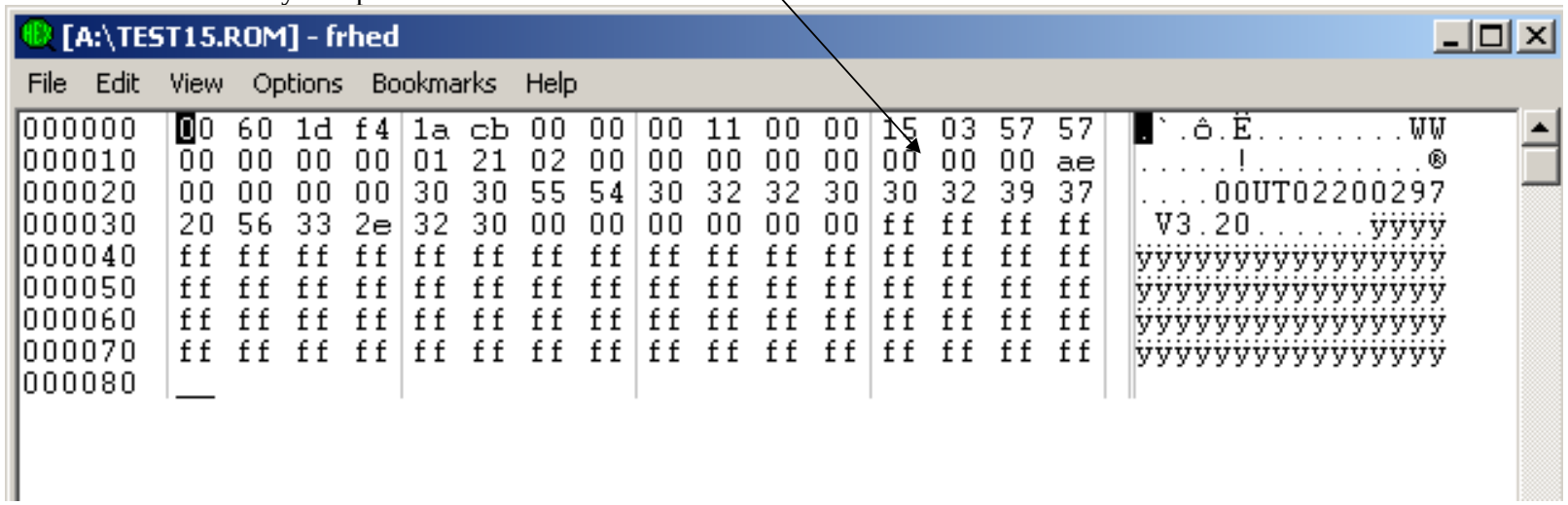
Uma vez espetado a placa LAN com eeprom para ser hackeiado ao PC, em modo DOS Executar o programa rteeprom.exe que serve para extrair o ROM do EEPROM, gravar num disquete o ROM com comando:
Rteeprom s xxxxxxxx.rom

Leve o disquete à executar em PC com windows com o programa HEX Editor de sua preferência (eu usei frhed)

Editar as tabelas dos 6 bytes e introduzir o mac address, depois com uma calculadora científica em modo HEX somar toda essa fila menos as tabelas 13 e 14, exemplo:

00 + 60 + 1d + f4 + 1a + cb + 11 + 57 + 57 = 03 15 -> 15 03 (checksum)

o resultado inverter os bytes e preencher as tabelas numero 13 e 14



The six bytes of the IEEE station address occupy the first six locations of the Address PROM space. The next six bytes are reserved. Bytes 12 and 13 should match the value of the checksum of bytes 1 through 11 and 14 and 15. Bytes 14 and 15 should each be ASCII “W” (57h). The above requirements must be met in order to be compatible with AMD driver software. APROMWE bit (BCR2, bit 8) must be set to 1 to enable write access to the Address PROM space.

Depois de isso salvar o arquivo com o nome yyyyyyyy.rom

Leve ao PC onde tem a placa LAN com eeprom e execute:
rteeprom p yyyyyyyy.rom

depois para asegurar que gravou sem erro, extraia num arquivo a imagem ROM e verifique com programa HEX Editor e se coincide com yyyyyyyy.rom:
rteeprom s zzzzzzzz.rom

yyyyyyyy.rom = zzzzzzzz.rom ? OK

Tire o eeprom e solde de volta ao equipo WPII ou AP-1000

Para apagar o firmware de Access Point e carregar o firmware de turbocell, vc precissa deixar no modo Forced Mode:
ao iniciar o equipo espere 3 segundos e aperte o botão reload por 30 segundos até que a luz do power fique laranjado.

E agora verificar se tem o mac address que lhe designou com OR-Manager ou Karlnet Configurator e carregue o firmware
OR-1X00_v415.bin + arquivo LKF da licença.