Ejercicio 3. Sniffer, Objetivo: **Utilizar un sniffer e interpretar el tráfico de red.**

Herramientas:

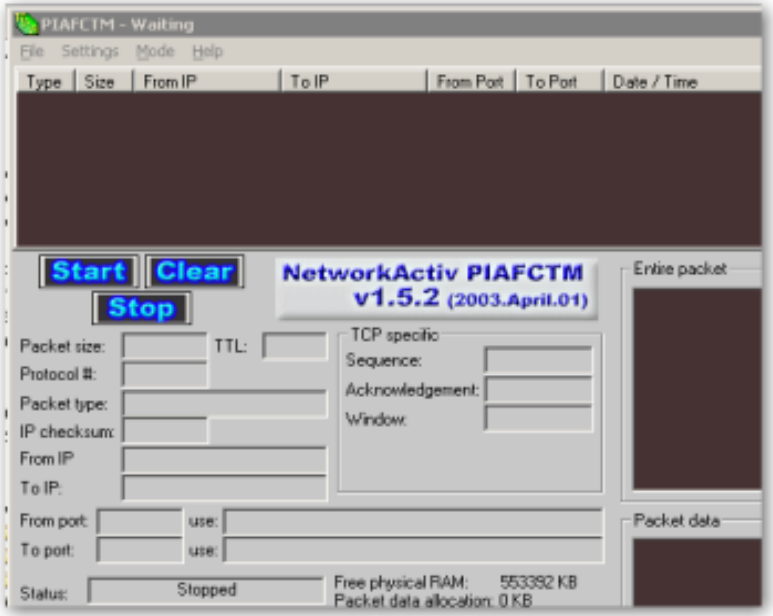
Wireshark,

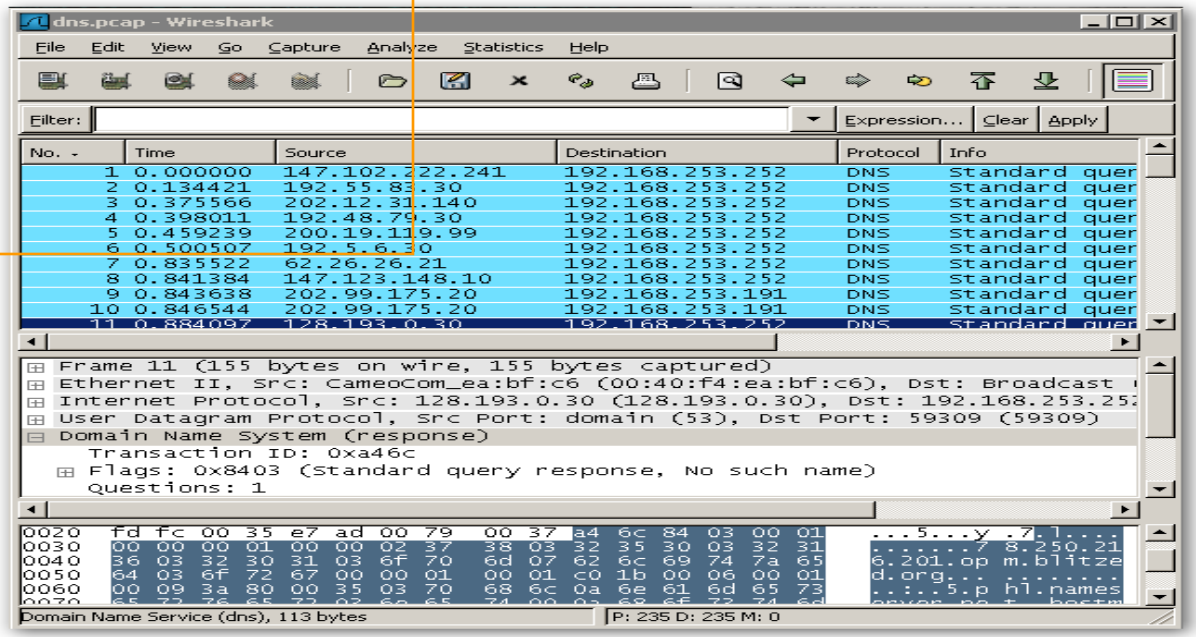
Winpcap

Networkactiv http://www.networkactiv.com/

Tareas

1. Instalar winpcap y reiniciar el equipo.
2. Instalar los Sniffers
3. Correr los Sniffers e interpretar el tráfico, (identificar rangos de ip validos, protocolos, mac adress, etc).





(documentar las salidas a un txt).

Ejercicio 4. Google Hacking. Objetivo: **Analizar ejemplos de ingeniería social, archivos confidenciales , archivos de configuración, información de reconocimiento**

Herramientas: www.google.com

•Reconocimiento, identificar sistema operativo y servicio web. **Ej intitle:"powered by Apache"**

•Paraíso del spammer, buscar ***.pst, ¨fw:¨, etc.**

•Listar directorios:

intitle:index.of "Back Up"

intitle:index.of.admin

intitle:index.of ws_ftp.log

•Buscar Archivos específicos:

inurl:cuentas filetype:xls

filetype:bak inurl:"passwd"

"access denied for user" "using password"

filetype:pst inurl:pst

•Ingeniería Social, buscar información útil para el atacante de un objetivo específico. (ej: busco información @algundominio.com)

- Buscar dispositivos específicos:

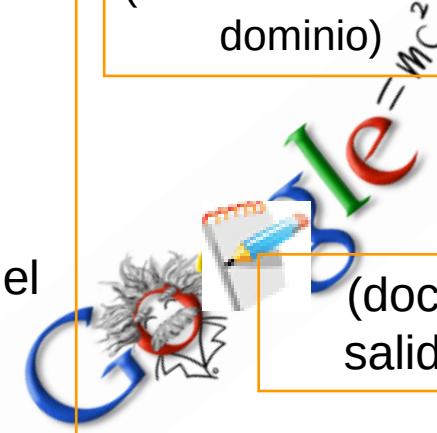
inurl:indexFrame.shtml Axis

intext:centreware inurl:status

- Buscar cuentas de correo electrónico:

@dominio.com

(encontrar 10 cuentas del dominio)



(documentar las salidas a un txt).