Análisis de malware

Análisis dinámico básico

Gustavo Romero López - gustavo@ugr.es

Updated: 3 de marzo de 2025

Departamento de Ingeniería de Computadores, Automática y Robótica

Por donde vamos...

Parte 1: Análisis básico

- Capítulo 1: Técnicas estáticas básicas
- Capítulo 2: Análisis de malware en máquinas virtuales
- Capítulo 3: Análisis dinámico básico

Parte 2: Análisis estático avanzado

- Capítulo 4: Curso intensivo de ensamblador x86
- Capítulo 5: IDA Pro
- Capítulo 6: Reconocimiento de construcciones de C en ensamblador
- Capítulo 7: Análisis de programas maliciosos para Windows

Parte 3: Análisis dinámico avanzado

Parte 4: Funcionalidad del malware

Parte 5: Anti-ingeniería inversa

Parte 6: Temas especiales

Lo que ya sabéis hacer...

Análisis estático:

- Identificar ficheros: MD5, SHA1, SHA256,...
- Antivirus: www.virustotal.com
- Detección de empaquetado: PEid y UPX
- Cadenas: strings
- Formato PE:
  - PEview
  - Depends
  - objdump
  - Resource Hacker
- Desensamblado: IDA Pro

Lo que os falta por aprender...

Análisis Dinámico:

- Entorno seguro
  - sandbox: Cuckoo, Joe Sandbox, Microsoft Sandbox
  - máquina virtual: Gnome Boxes, VMware, VirtualBox
- Process Monitor
- Process Explorer
- Regshot
- ApateDNS + INetSim
- Wireshark
- Depuración:
  - OllyDbg/Immunity Debugger: modo usuario
  - Windbg: modos usuario y núcleo

Motivación

- Examen de la ejecución del malware.
- El análisis estático puede acabar en un callejón sin salida...
  - ofuscado/empaquetado/cifrado
  - conocimientos insuficientes/exceso de dificultad
- Observar el comportamiento del malware puede ser más eficaz y sencillo.
- Podemos hacerlo de dos formas:
  - En vivo: monitorizar mientras se ejecuta.
  - A posteriori: comparar el sistema antes y después.
- La mejor forma de averiguar que hace el malware.
- Usar sólo después de un análisis estático básico.

Entorno aislado ("*SandBox*")

- Definición: mecanismo de seguridad para ejecutar programas en un entorno seguro.
- Mejor cuanto más se parezca a un sistema real
- Automatizan el proceso de rastreo de actividad y elaboran informes sobre el comportamiento del malware.
- Ejemplos:
  - Cuckoo: https://cuckoosandbox.org/`https://cuckoo.cert.ee`
  - Joe Sandbox: https://www.joesecurity.org
  - Microsoft Sandbox
- Inconvenientes:
  - pueden ser detectados
  - vulnerabilidades en el anfitrión
  - sin opciones desde el intérprete de órdenes
  - sin interacción de red
  - diferencias con un sistema real: entorno, registro,...

Entorno aislado ("*SandBox*")

- Permite observar el la actividad del malware sobre....
  - procesos/hebras
  - sistema de ficheros
  - mutex
  - registro
  - red
  - antivirus
- Inconvenientes:
  - no utiliza opciones de línea de órdenes
  - no registra todos los eventos por falta de tiempo
  - puede ser detectado por el malware
  - comportamiento anómalo por diferencias con un sistema real
  - no lanzamiento de DLLs
  - falta de conclusiones precisas

Ejecución de malware

Ejecutables (*.exe):

- doble click desde un interfaz gráfico
- ejecución desde el intérprete de órdenes:

```
c:\virus.exe
```

Bibliotecas de enlace dinámico (*.dll):

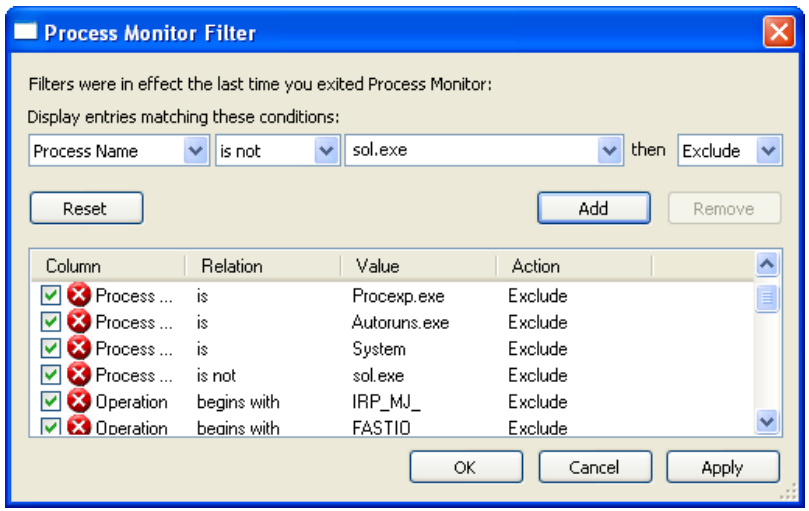
- `c:\>rundll32.exe rip.dll, Install`
- Convertir DLL en ejecutable cambiando su cabecera
- Instalar DLL como un servicio y ejecutarlo

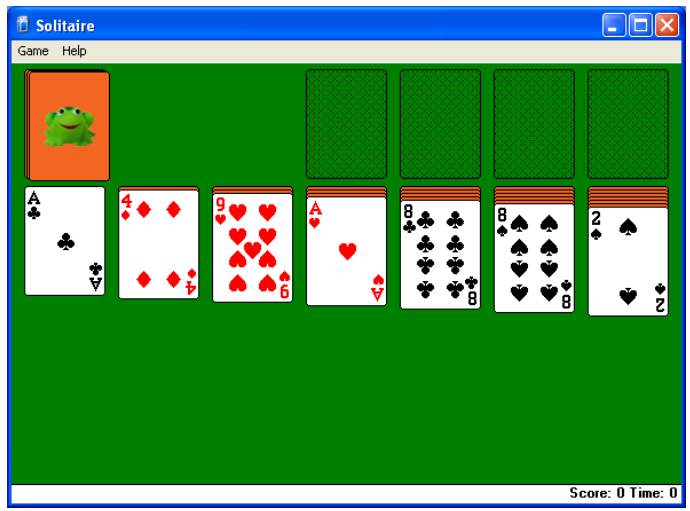
```
c:\>rundll32.exe iprx32.dll, InstallService ServiceName
c:\>net start ServiceName
```

Process Monitor

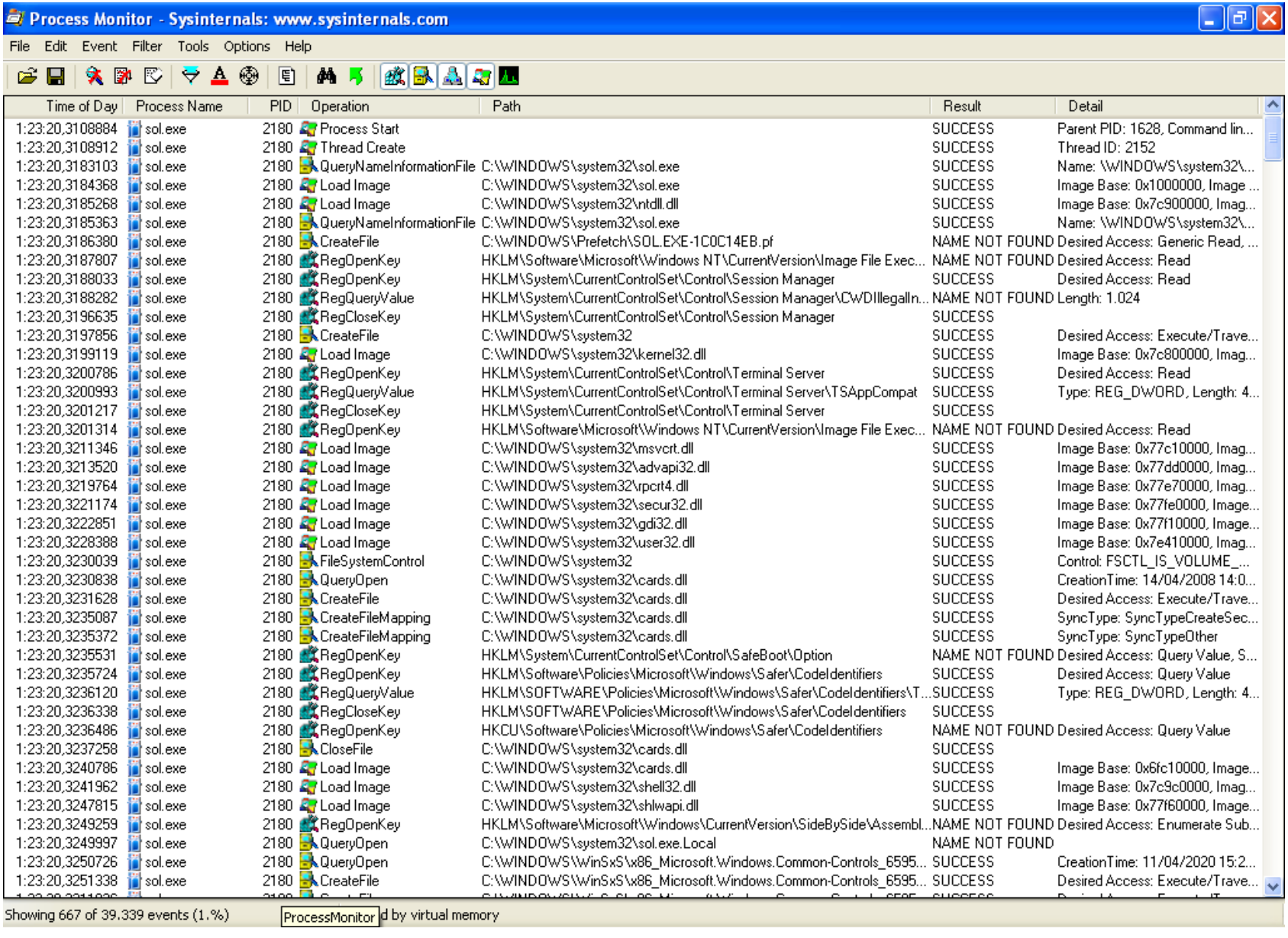
- Monitoriza: registro, sistema de ficheros, red y procesos.
- Genera tanta información que es vital filtrarla.
- Ejercicio: ¿Que hace el solitario de Windows?
  1. Arranca Process Monitor
  2. Detener la captura de eventos
  3. Crea el filtro:

     "`Process Name is not sol.exe then Exclude`"
  4. Reactivar la captura de eventos
  5. Lanza el solitario





Process Monitor

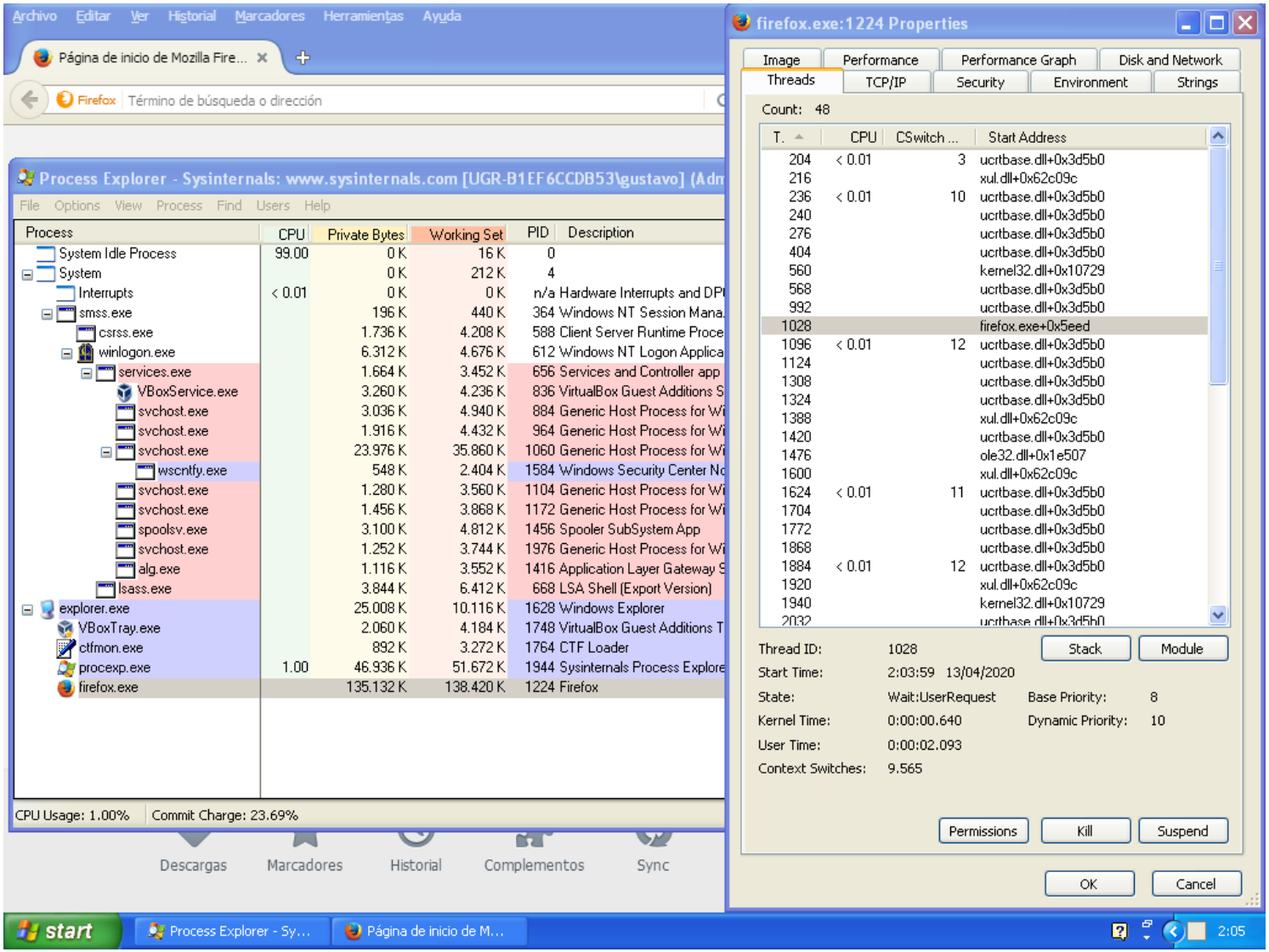


Process Explorer

- Gestor de tareas que permite analizar en detalle el uso que los procesos hacen del sistema.
- Identificación mediante colores:
  - servicios: rosa
  - procesos: azul
  - procesos nuevos: verde (temporal)
  - procesos finalizados: rojo (temporal)
- Opciones más interesantes:
  - Verificar: compara la imagen de un proceso en memoria con su original en disco (binarios firmados).
  - Comparar cadenas: diferencias sustanciales indicarían un reemplazo de proceso.
  - Utilizar Dependency Walker: localizar uso de DLLs.
  - Analizar documentos maliciosos: uso de recursos.

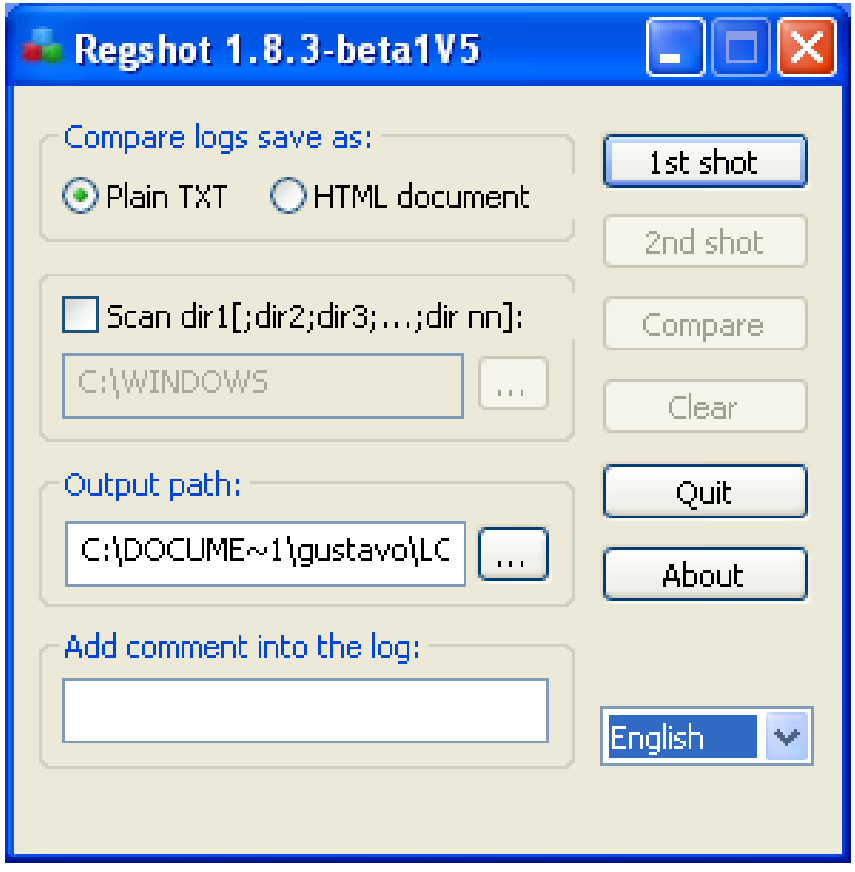
Process Explorer

- Ejercicio: ¿Cuántas hebras lanza Firefox?



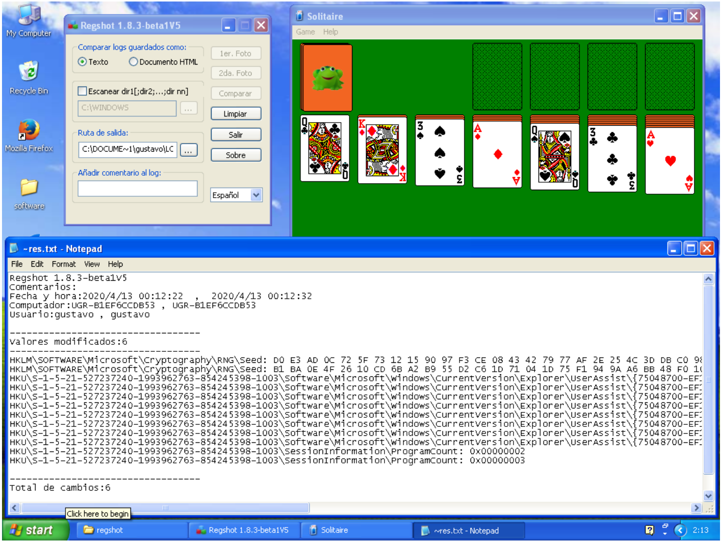
Comparando instantáneas del registro: Regshot

- Permite tomar y comparar instantáneas del registro.
- Uso:
  - 1º foto
  - ejecutar malware
  - 2ª foto
  - comparar



Comparando instantáneas del registro: Regshot

◎ Ejercicio: ¿Afecta el solitario al registro de Windows?

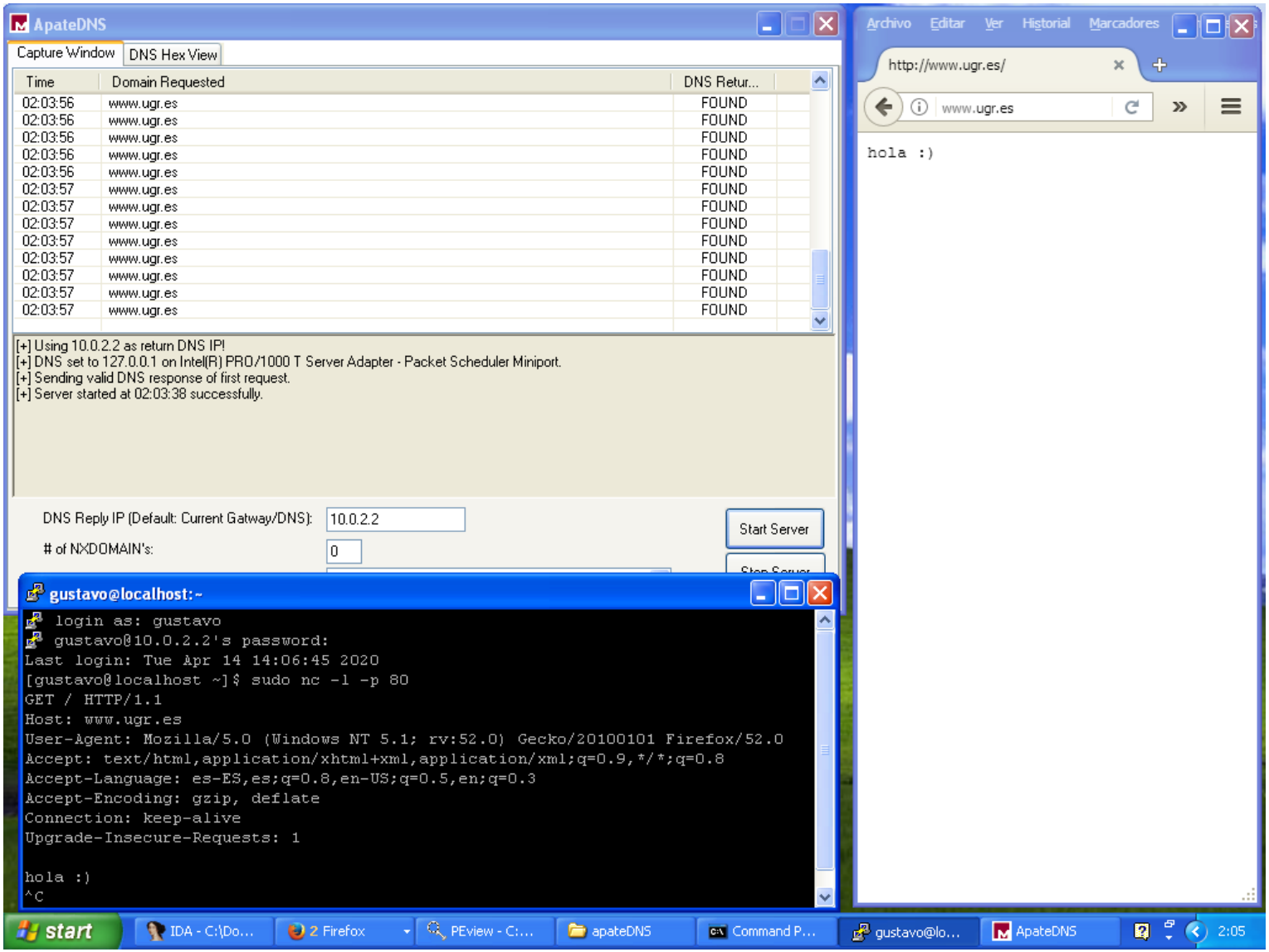


Simulando una red

- El malware suele comunicarse con servidores de control.
- Crear una red falsa permite obtener pistas:
  - DNSs
  - IPs
  - paquetes que utilizar como identificadores
- **ApateDNS**: servidor DNS bajo nuestro control.
- **Netcat**: la navaja suiza del TCP/IP.
  - stdin –> red
  - red –> stdout

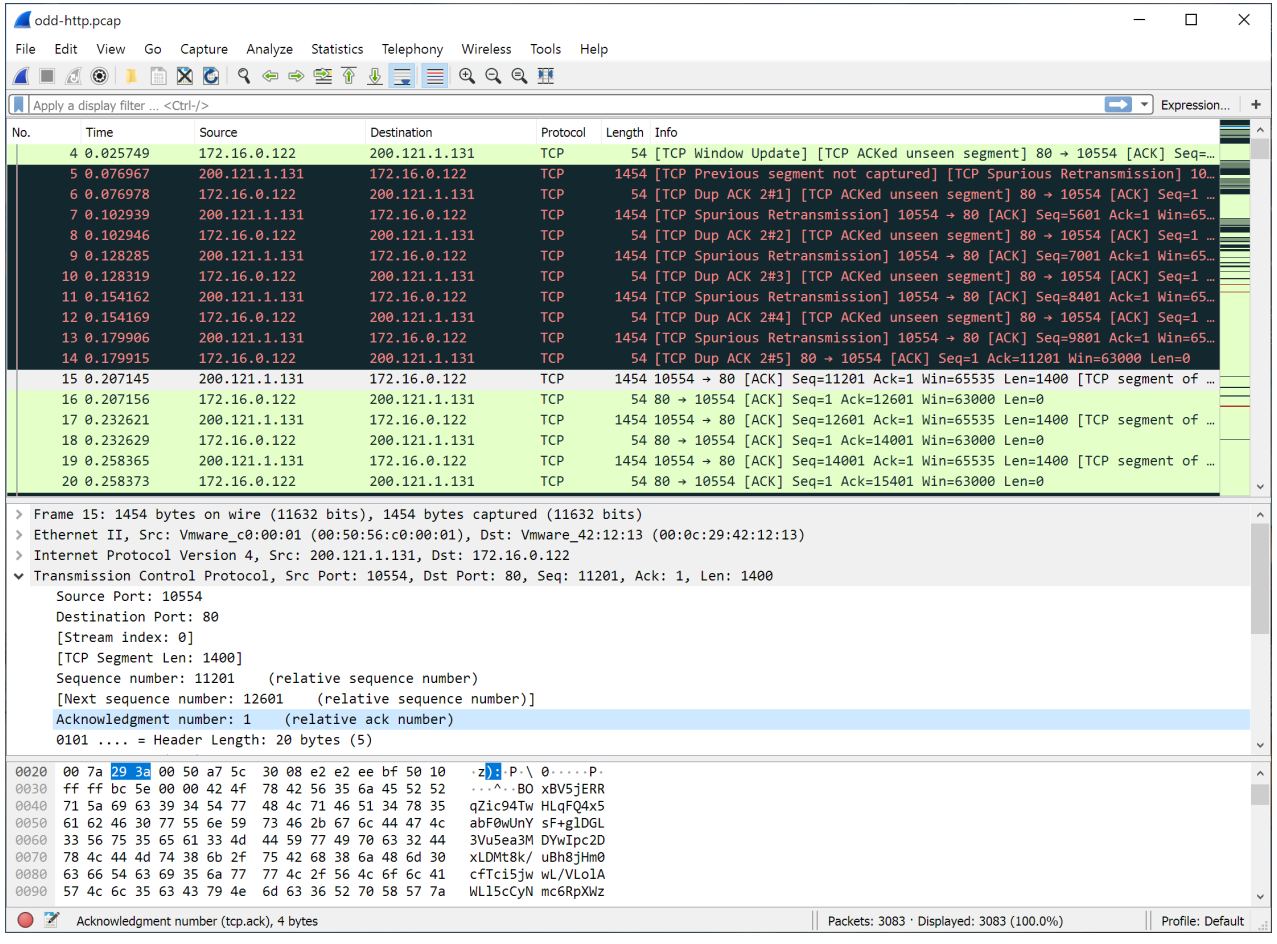
Trasteando en la red

- Ejercicio: Haga que la página web de la UGR le salude.

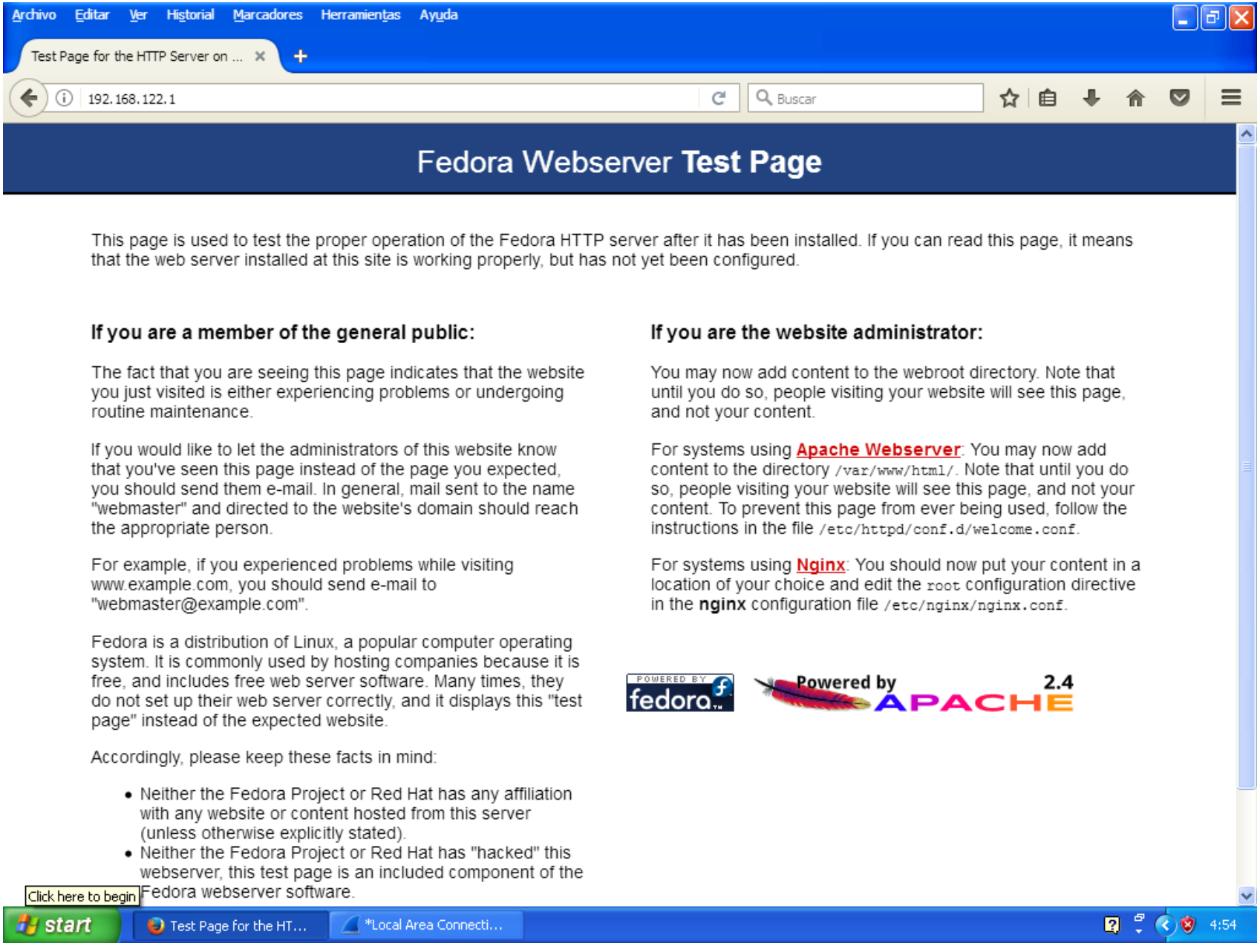


Capturando tráfico de red con Wireshark

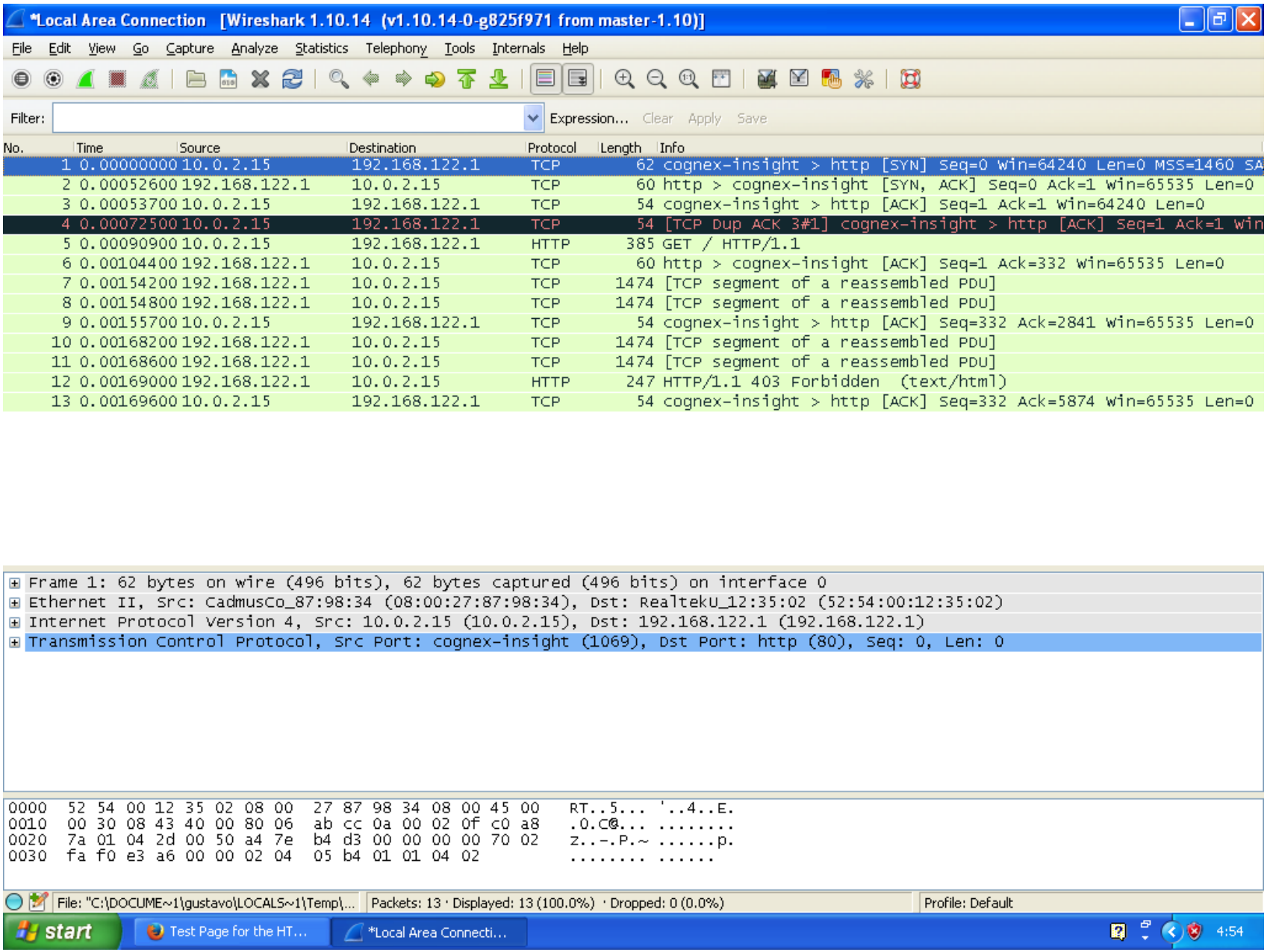
- Intercepta y almacena tráfico de red.
- Facilita la visualización y el análisis tanto de paquetes individuales como de intercambios secuenciados.



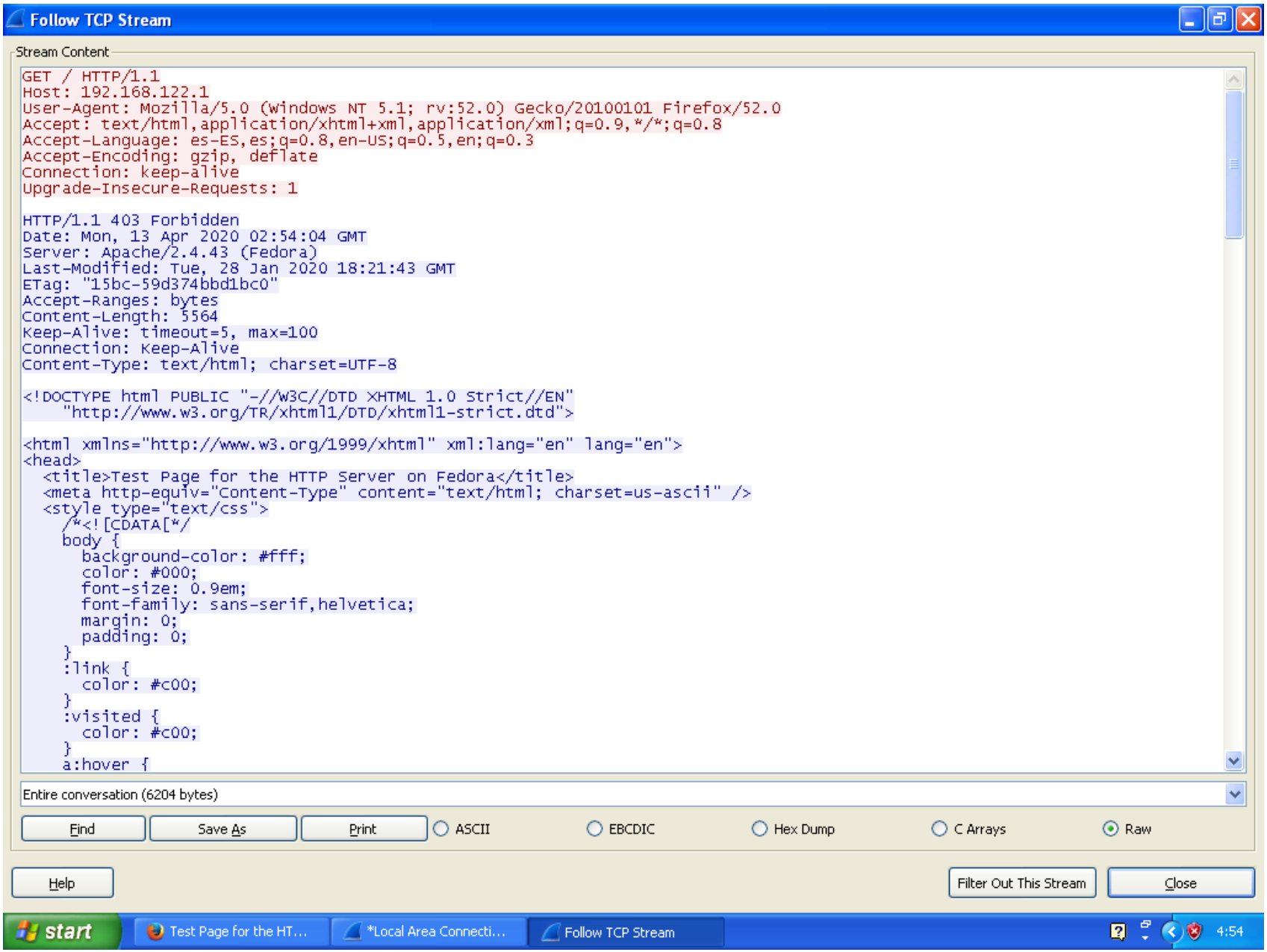
Wireshark: diálogo Firefox <–> HTTPD



Wireshark: diálogo Firefox <–> HTTPD



Wireshark: diálogo Firefox <–> HTTPD



INetSim

- Simulador de los servicios más comunes de Internet.
- Servicios emulados: DNS, FTP, HTTP, HTTPS, IRC, POP, POP3, SMTP,...
- Simular el comportamiento de los servidores reales para intentar mantener al malware funcionando.
- Registra todas conexiones y peticiones entrantes.

En resumen...

1. Process Monitor
2. Process Explorer
3. Regshot
4. ApateDNS + nc/FakeNet/INetSim
5. Wireshark

... o todo a la vez desde una caja de arena...

Prácticas

1. Lab03-01.exe:
   - 1.1 ¿Qué funciones importa? ¿Qué cadenas contiene?
   - 1.2 ¿Deja señales en el anfitrión (*host-based indicators*)?
   - 1.3 ¿Hay firmas de red? ¿Cuáles?

2. Lab03-02.dll:
   - 2.1 ¿Puede conseguir que se instale?
   - 2.2 ¿Cómo hacer que se ejecute?
   - 2.3 ¿Cómo encontrar el proceso bajo el que se ejecuta?
   - 2.4 ¿Qué filtros usaría en `procmon` para extraer información?
   - 2.5 ¿Qué rastros deja en el anfitrión?
   - 2.6 ¿Hay firmas de red?