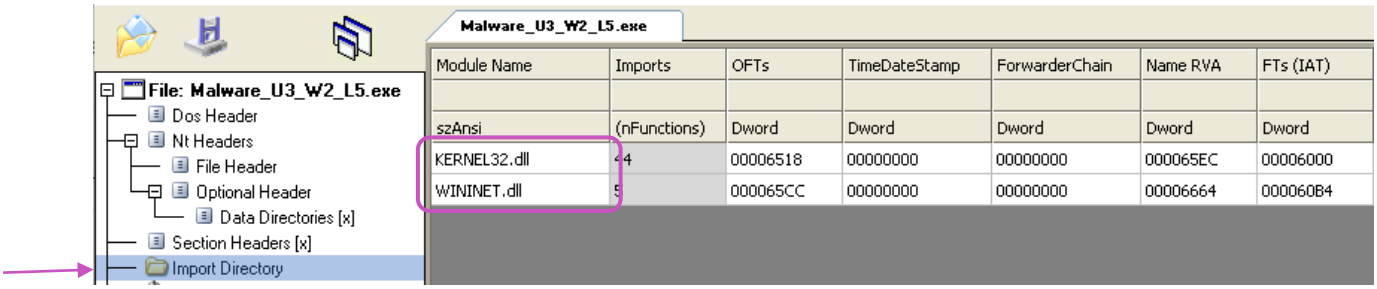
Analisi statica e dinamica: Un approccio pratico

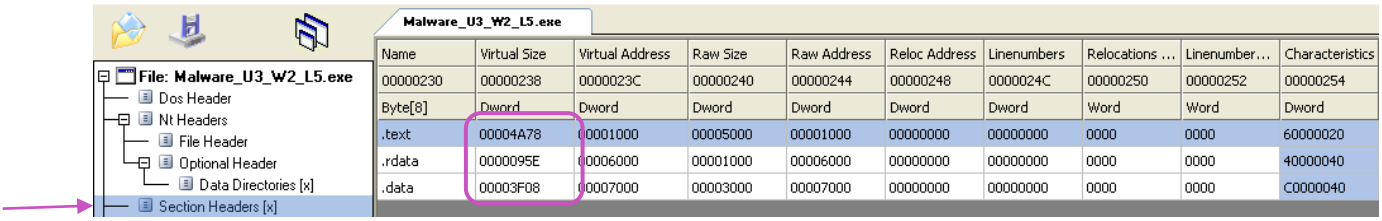
Esaminare il file **Malware_Pratico_u3_W2_L5:**

1. Quali **librerie** vengono importare dal file eseguibile? Fare anche una descrizione.
   Usando il tool **CFF Explorer** presente sulla macchina dedicata all'analisi dei malware, scegliamo il file da esaminare controlliamo le librerie importate selezionando dal menu **Import directory:**



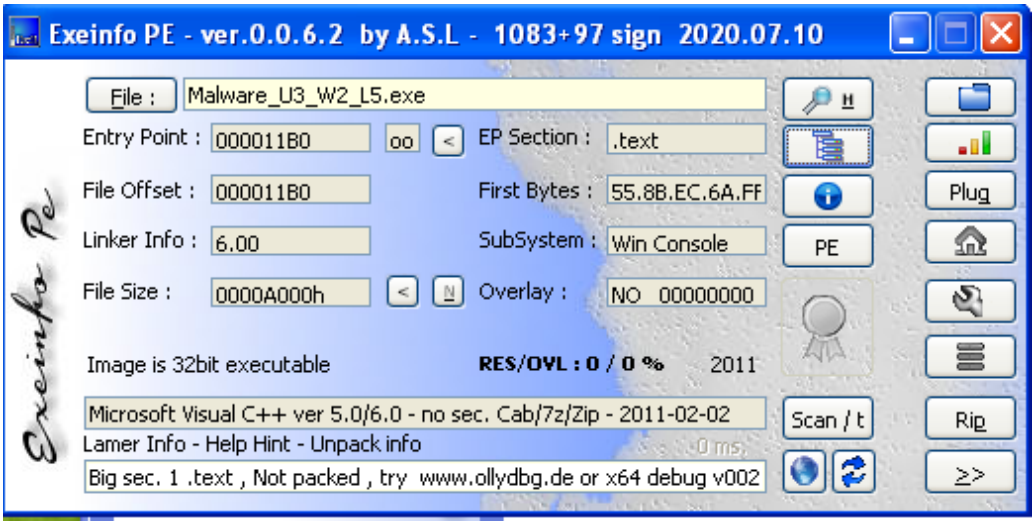
   Le librerie presenti sono:
   - **Kernel32.dll**: è una libreria di sistema fondamentale per i sistemi operativi Windows. Contiene un insieme di funzioni che consentono l'interazione con il sistema operativo e la gestione delle risorse di base. Ad esempio la gestione dei file, dei processi e dei thread, della memoria, sincronizzazione e segnalazione degli eventi.
   - **Wininet.dll**: è una libreria di sistema che fornisce funzionalità di rete per i sistemi operativi Windows. Essa include funzioni per l'implementazione di protocolli di rete come HTTP, FTP e NTP. Ad esempio offre funzioni per l'accesso e la comunicazione tramite protocolli di rete, permette di eseguire operazioni di download e upload di file, gestire i cookie e le cache dei file temporanei.

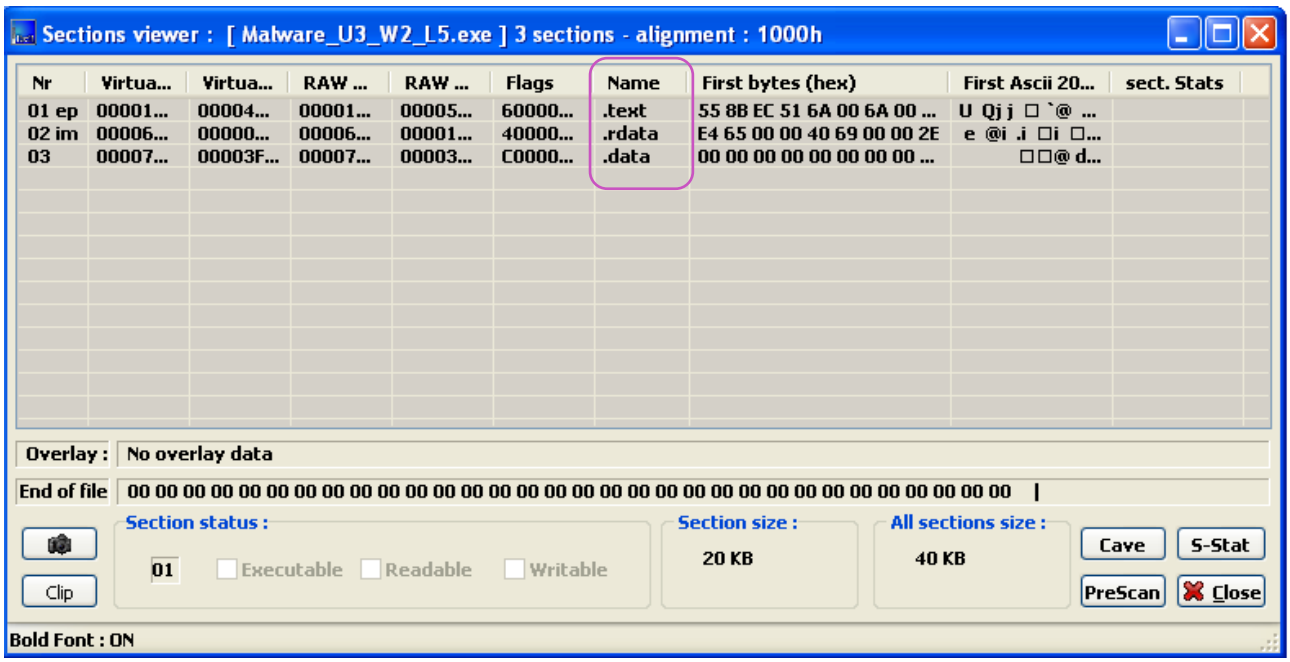
2. Quali sono le **sezioni** di cui si compone il file eseguibile del malware? Fare anche una descrizione
   Con lo stesso tool **CFF Explorer** possiamo controllare anche di quali sessioni compongono il file in esame, selezionando dal menu **Section Headers:**



   Le sezioni presenti sono:
   - **.text**: contiene le istruzioni di codice che la CPU eseguirà una volta che il software sarà avviato. Questa sezione rappresenta il nucleo del programma, in quanto contiene il codice effettivo che viene eseguito per svolgere le operazioni desiderate. È la sezione principale che viene eseguita dalla CPU, poiché contiene le istruzioni che determinano il comportamento del programma.
   - **.rdata**: (read-only data) contiene principalmente dati di sola lettura utilizzati dall'eseguibile. Questa sezione contiene solitamente costanti, tabelle di lookup o altre informazioni di sola lettura che vengono utilizzate dal programma durante l'esecuzione. Il contenuto di questa sezione non può essere modificato durante l'esecuzione del programma.
   - **.data**: contiene dati inizializzati e variabili globali del programma eseguibile. Questa sezione include dati che possono essere letti e scritti durante l'esecuzione del programma. Ad esempio, può contenere variabili globali, variabili statiche e altri dati inizializzati che possono essere modificati durante l'esecuzione del programma.

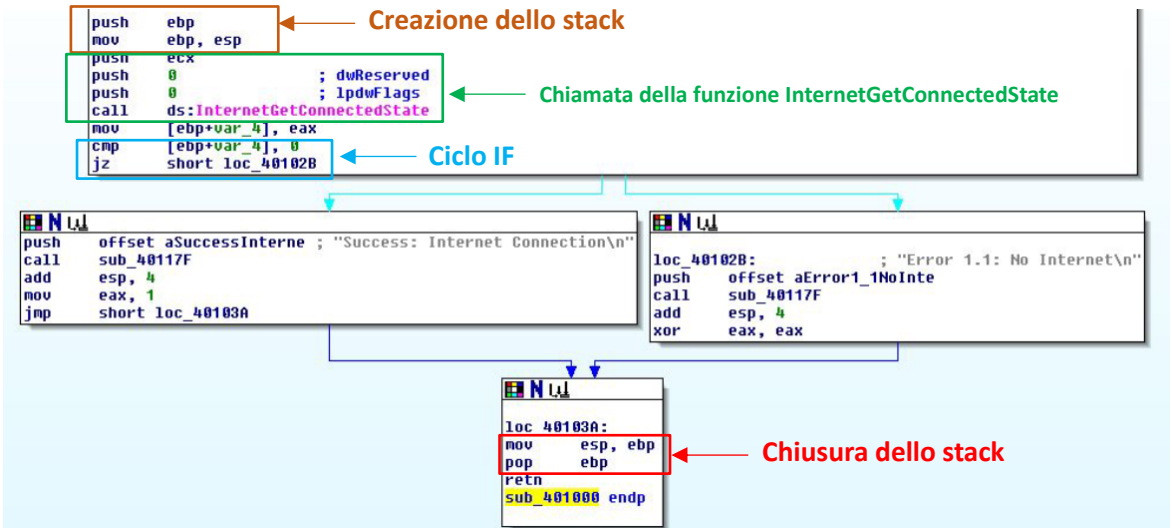
Lo stesso risultato si può osservare anche usando il tool ExeinfoPE:





Con riferimento alla figura in slide 3, rispondere ai seguenti quesiti:

3. Identificare i **costrutti** noti (creazione dello stack, eventuali cicli, altri costrutti)



4. Ipotizzare il comportamento della funzionalità implementata
   Dopo la creazione dello stack, viene chiamata la funzione **InternetGetConnectedState** per cui vengono passati con push i tre parametri che gli sono necessari, questa particolare funzione serve a verificare se la connessione internet è presente o meno sulla macchina target.
   Successivamente con un ciclo IF, si compara (cmp) il valore della var_4 con 0, perché in caso siano uguali tra loro allora lo Zero Flag ZF è 0, in caso la comparazione invece rilevi che sono diversi lo ZF sarà 1. La funzione **jz** prevede il salto alla locazione di memoria specificata se ZF=1, in questo caso alla loc_40102B, se ZF=0 allora vuol dire che la connessione è attiva.
   Finito il compito dello stack si può chiudere, e ritornare (retn) al punto di chiamata e riportando il valore del puntatore ESP al suo valore originario.

   Il malware potrebbe sfruttare la connessione ad internet per eseguire altre operazioni non presenti in questo codice, si può ipotizzare che in presenza di connessione internet e avendo accesso ai dati della macchina target può raccogliere informazioni sul sistema operativo, della rete, dati personali e sensibili, creando una connessione con un server di controllato dall'attaccante può inviare tali dati, il malware potrebbe creare una backdoor per consentire una comunicazione tra macchina vittima e attaccante o infettare altre macchine ad essa collegate.

5. Dopo il bonus, spiegare quale istruzione assembly complessa

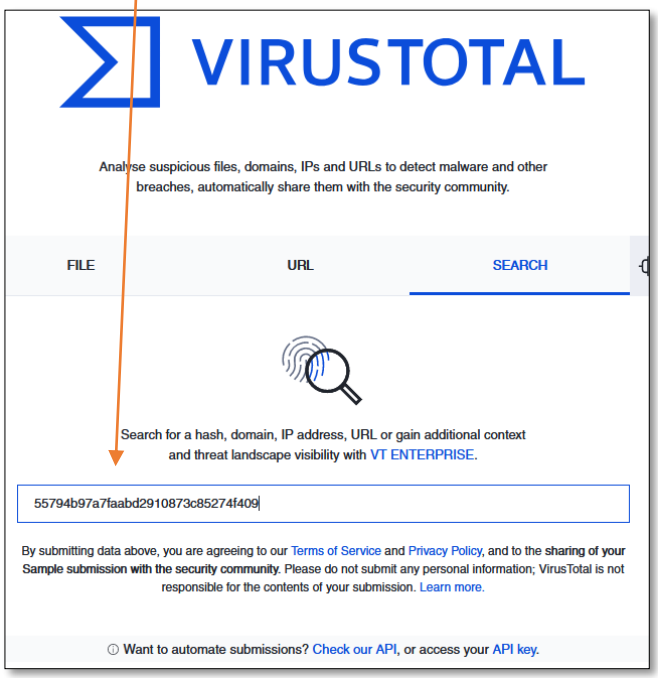
BONUS:

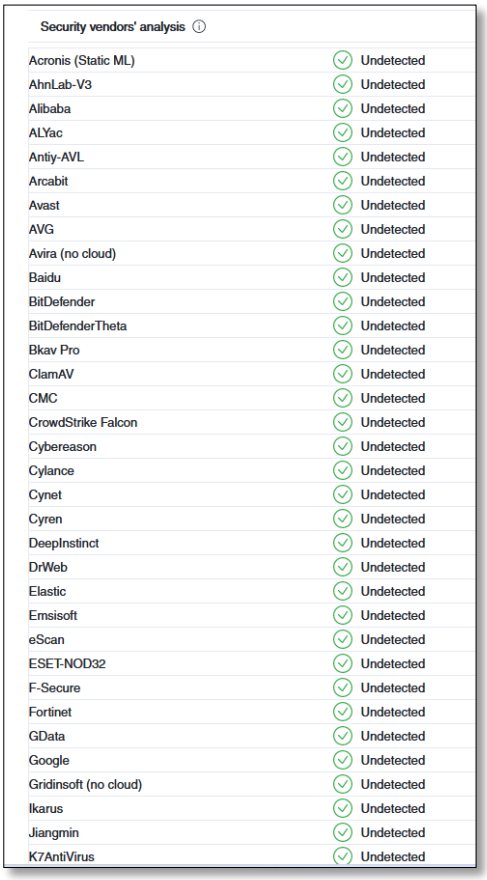
Un giovane dipendente neo assunto segnala al reparto tecnico la presenza di un programma sospetto.
Il suo superiore gli dice di stare tranquillo ma lui non è soddisfatto e chiede supporto al SOC.
Il file “sospetto” è IEXPLORE.EXE contenuto nella cartella C:\Program Files\Internet Explorer
Come membro senior del SOC ti è chiesto di convincere il dipendente che il file non è maligno.
Possono essere usati gli stumenti di analisi statica e/o analisi dinamica basica visti a lezione.
No disassembly no debug o similari
Virus Total non basta, non basta dire iexplorer è Microsoft è buono.

- Senza avviare il file “sospetto” si può calcolarne l’hash, Utilizza un tool come md5deep per calcolare l'hash, un codice alfanumerico univoco che rappresenta l'integrità del file, e poi inserirlo su VirusTotal, un servizio che analizza i file con più di 70 motori antivirus e altre tecnologie di scansione per individuare eventuali segnalazioni di malware. non vengono rilevate segnalazioni negative o indicazioni di malware dai motori antivirus e dalle altre tecnologie di scansione, questo suggerisce che il file "IEXPLORE.EXE" non è stato identificato come maligno dai fornitori di sicurezza rappresentati su VirusTotal.

```
C:\Documents and Settings\Administrator\Desktop\md5deep-4.3>md5deep "C:\Program
Files\Internet Explorer\IEXPLORE.EXE"
55794b97a7faabd2910873c85274f409  C:\Program Files\Internet Explorer\IEXPLORE.EX
E
```

-





- Possiamo andare a controllora le librerie che importa usando CFF Explorer:

MSVCRT: contiene funzioni di runtime per applicazioni scritte in linguaggio C o C++. Gestisce l'allocazione della memoria, le operazioni di input/output, le funzioni matematiche e altro ancora.

Kernel32: contiene funzioni per l'interazione con il sistema operativo Windows. Gestisce operazioni di sistema come la manipolazione dei file, la gestione della memoria, la creazione dei processi e dei thread.

User32: gestisce l'interfaccia utente di Windows. Fornisce funzioni per la creazione e la gestione delle finestre, la gestione degli eventi di input, il rendering grafico e altre funzionalità dell'interfaccia utente.

Shlwapi: fornisce funzioni di utilità legate all'interfaccia utente, operazioni di file e gestione delle stringhe.

SHDOCVW supporta la visualizzazione di documenti come pagine web e file HTML. Offre funzionalità di rendering e gestione dei documenti HTML.

Queste librerie offrono funzionalità di runtime, interazione con il sistema operativo, gestione dell'interfaccia utente, utilità per operazioni di file, manipolazione delle stringhe e visualizzazione di documenti. Sono fondamentali per lo sviluppo e il funzionamento delle applicazioni Windows.

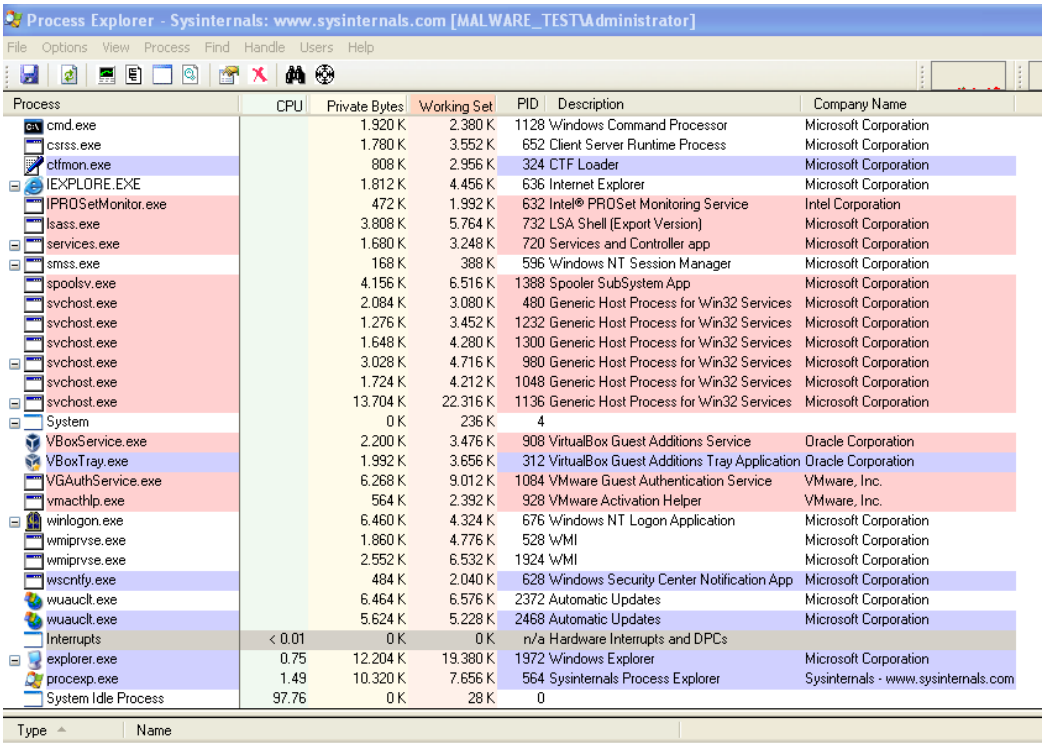
IEXPLORE.EXE

Module Name	Imports	OFTs	TimeDateStamp	ForwarderChain	Name RVA	FTs (IAT)
szAnsi	(nFunctions)	Dword	Dword	Dword	Dword	Dword
msvcrt.dll	1	00002830	FFFFFFFF	FFFFFFFF	0000284C	00001144
KERNEL32.dll	43	000026EC	FFFFFFFF	FFFFFFFF	00002B66	00001000
USER32.dll	16	000027EC	FFFFFFFF	FFFFFFFF	00002C8C	00001100
SHLWAPI.dll	16	000027A8	FFFFFFFF	FFFFFFFF	00002D30	000010BC
SHDOCVW.dll	2	0000279C	FFFFFFFF	FFFFFFFF	00002D3C	000010B0

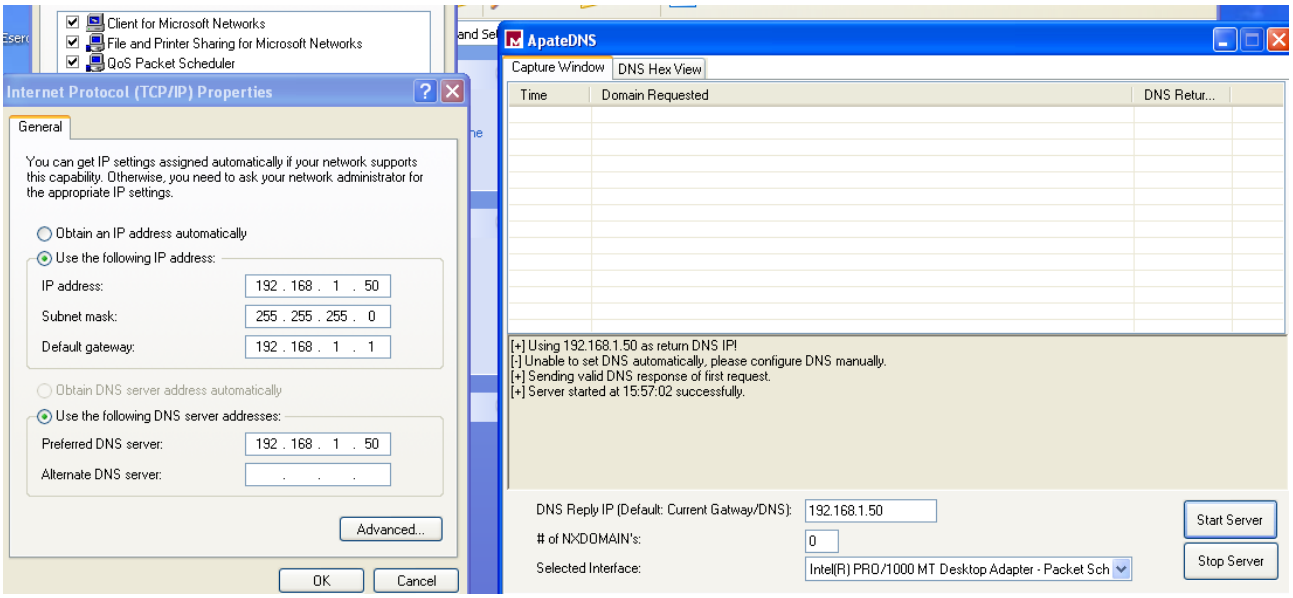
Proviamo quindi a eseguire un'analisi **dinamica basica**:

- Avviare Process Explorer
- Avviare il server DNS con ApateDNS
- Effettuare una prima istantanea con Regshot
- Avviare Process Monitor
- Avviare Wireshark
- Avviare il file eseguibili oggetto d'interesse
- Stoppare le catture Wireshark e Process Monitor
- Salvare una seconda istantanea con Regshot per notare eventuali modifiche del file eseguibili alle chiavi di registro
- Fermate il server di ApateDNS
- Fermare Process Explorer
- Controllare e analizzare i risultati

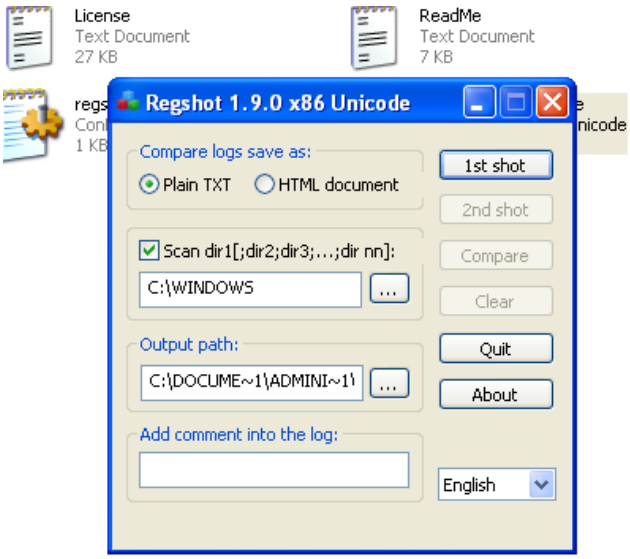
Process Explorer è un tool sviluppato da Microsoft Sysinternals che consente di analizzare dettagliatamente tutti i processi in esecuzione su un sistema operativo Windows.



Con ApateDNS intercettiamo le richieste che IEXPLORER.EXE effettua verso i domini internet, imposteremo il DNS uguale al nostri IP



Con **Regshot** si scatta una prima istantanea dello stato delle chiavi di registro



Process Monitor monitora i pro