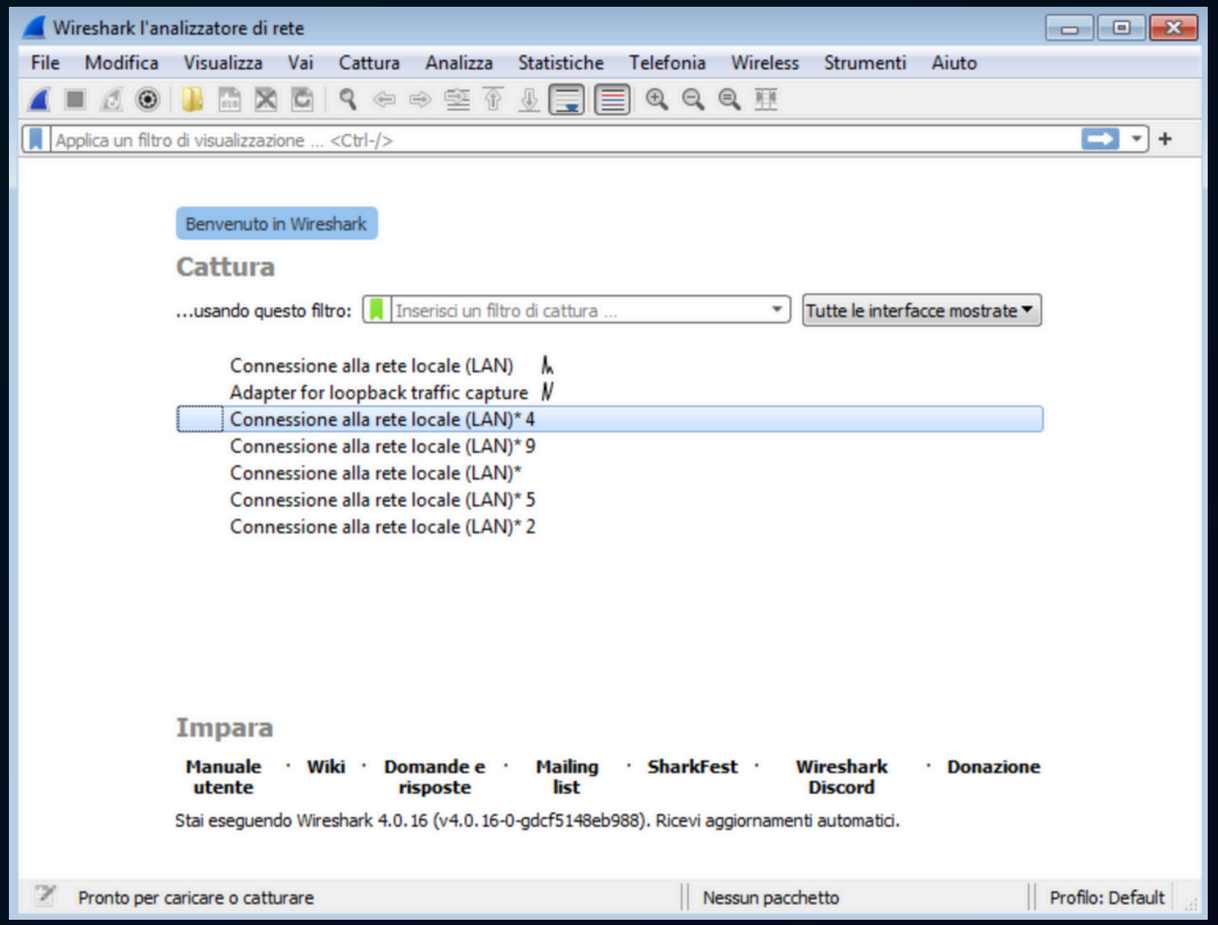
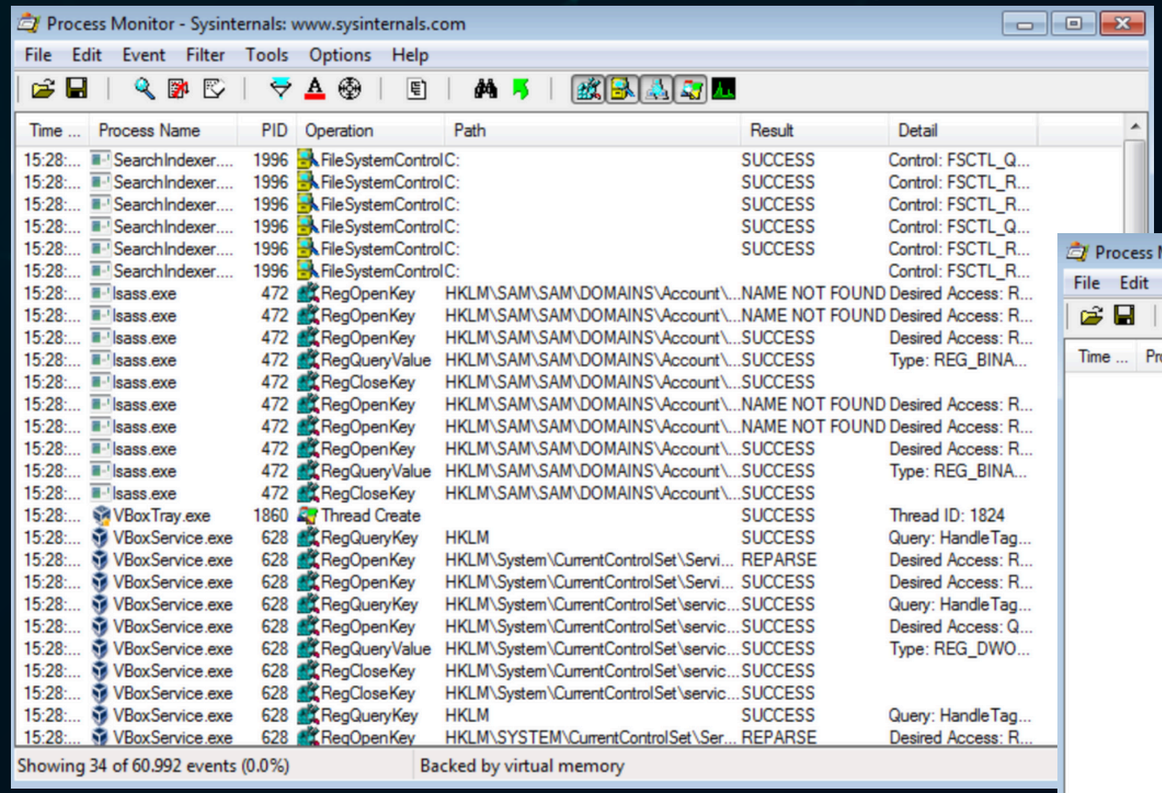
REPORT

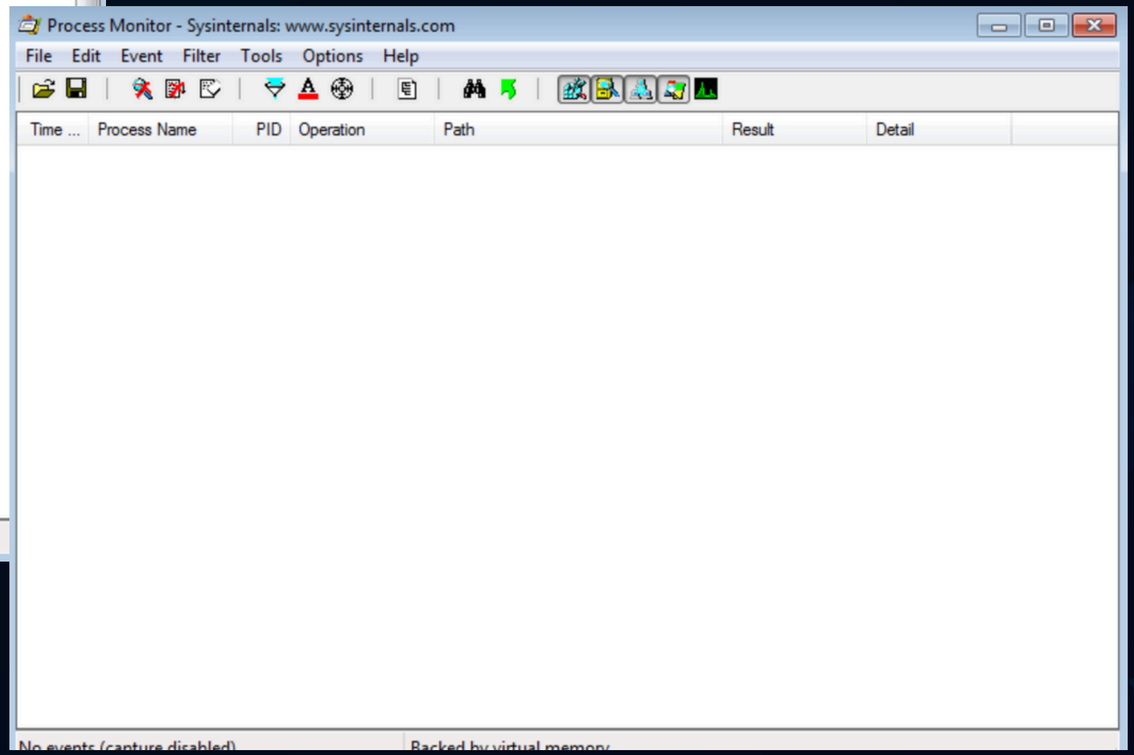
S10-L2

Prima di tutto avvio tutti i programmi necessari per l’analisi dinamica del malware
1-Wireshark

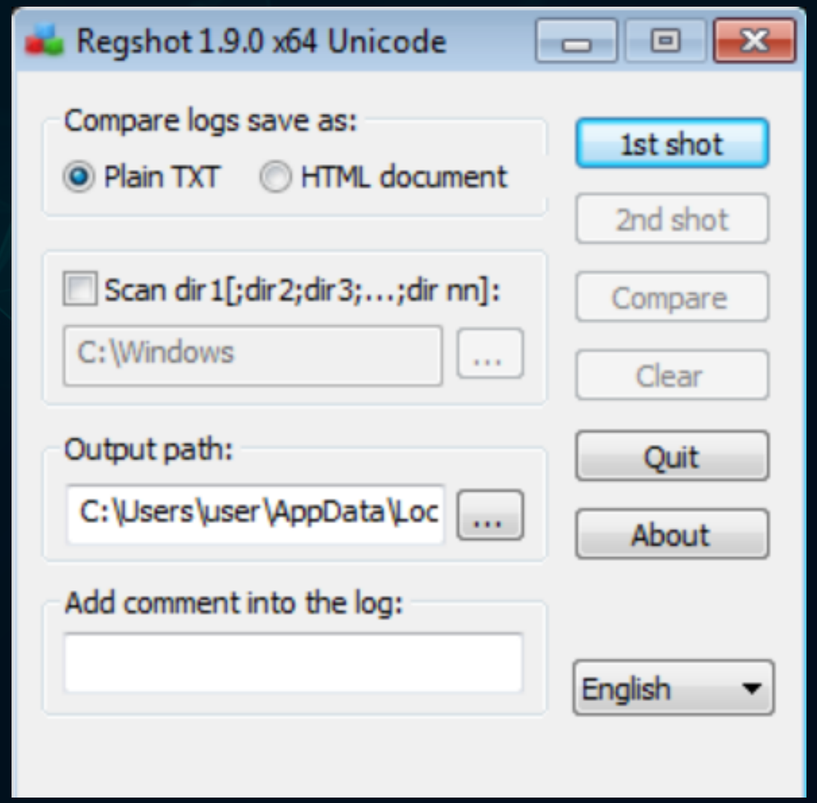


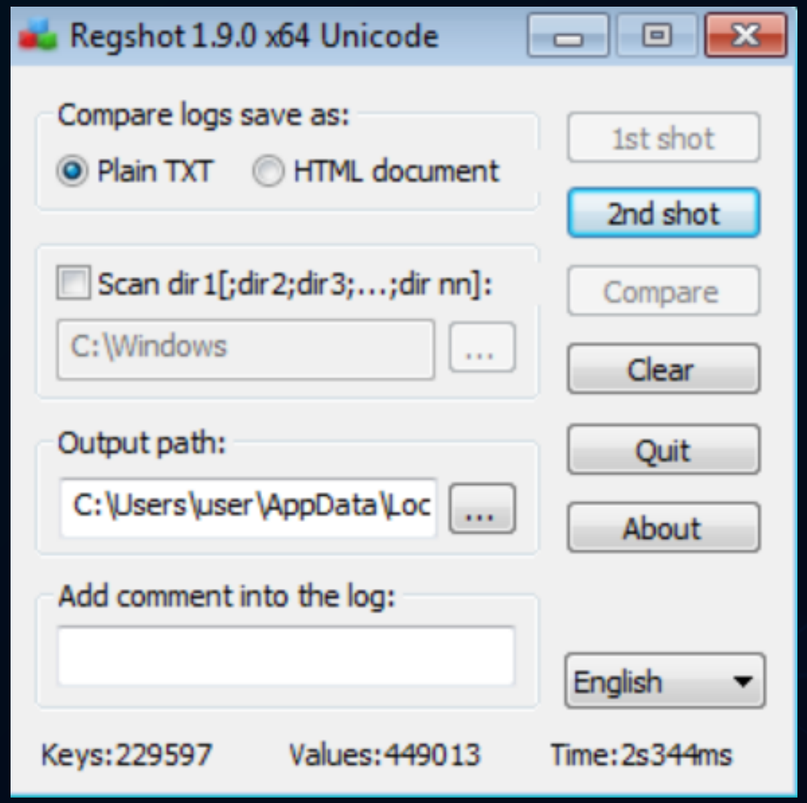
2-Apro Process Monitor, lo metto in pausa e faccio un clear, più avanti metterò dei filtri per filtrare solo quello che mi interessa



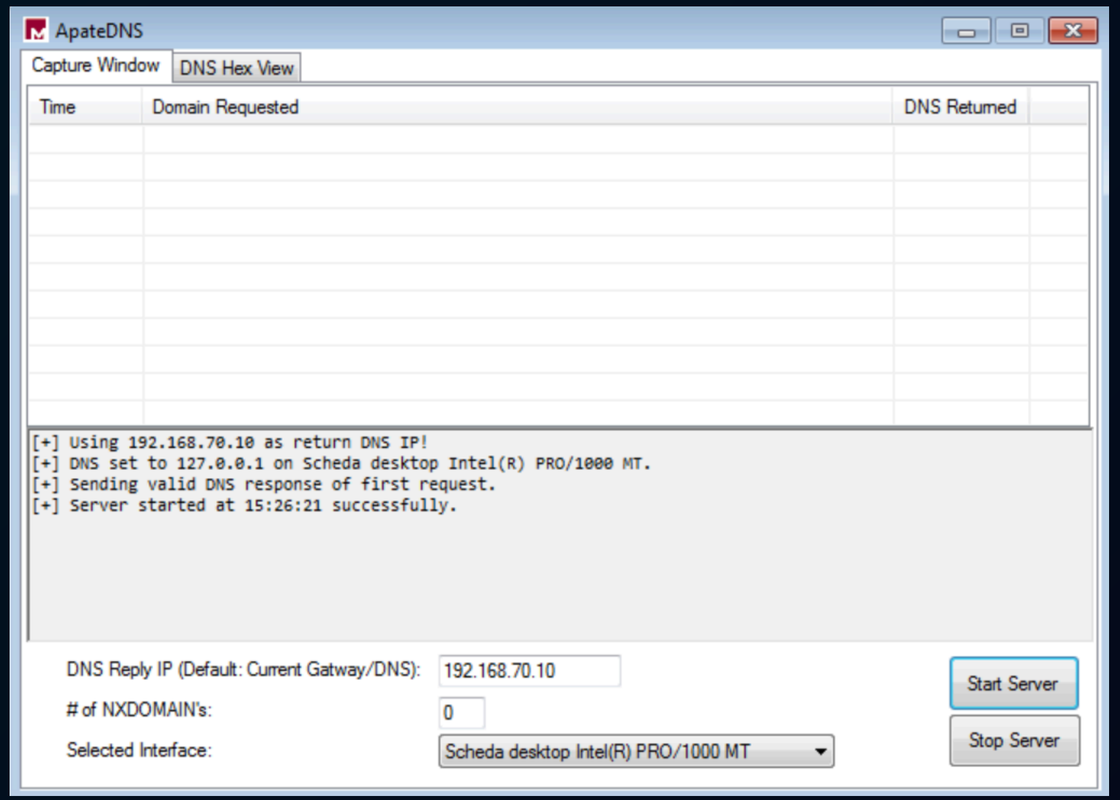


3-Apro Regshot e faccio una prima scansione delle chiavi e dei loro valori

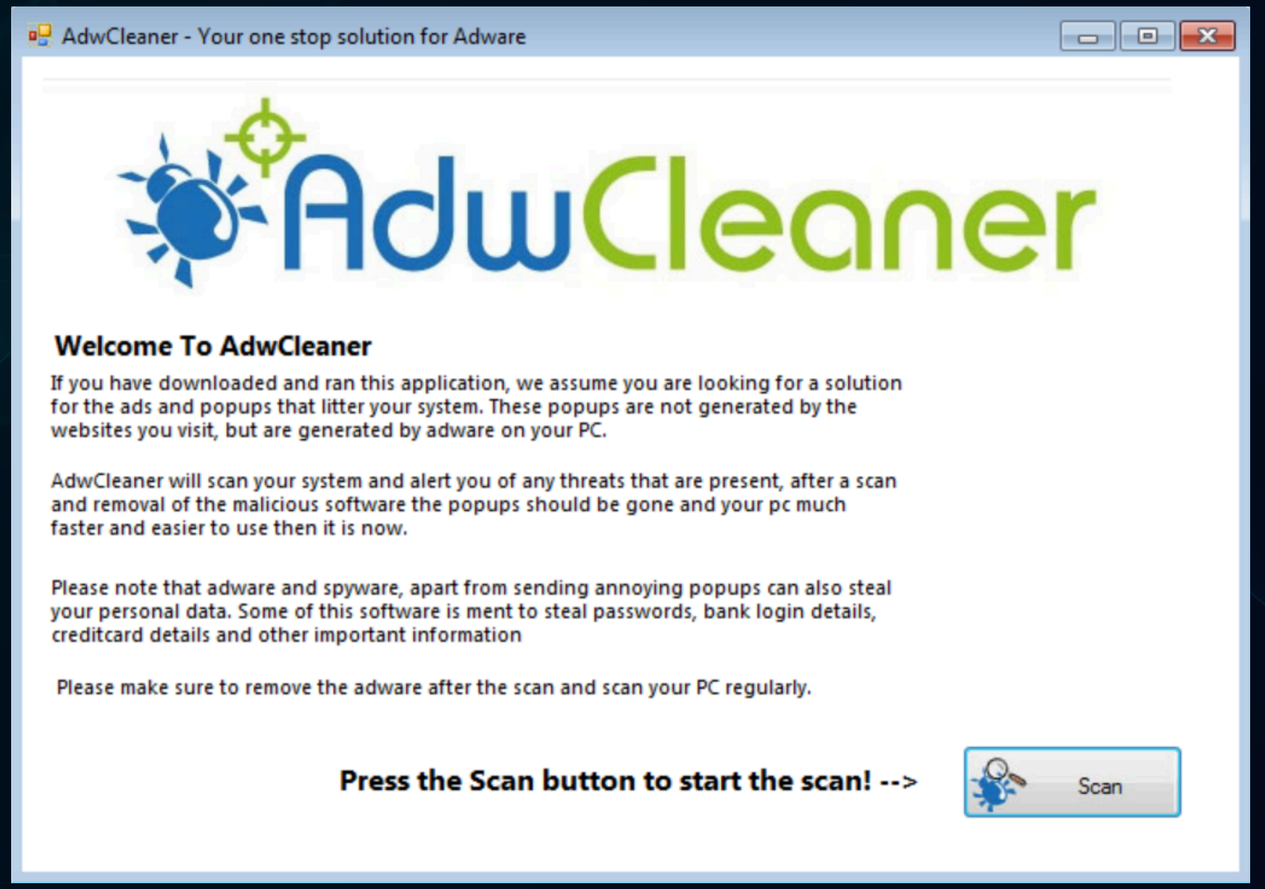


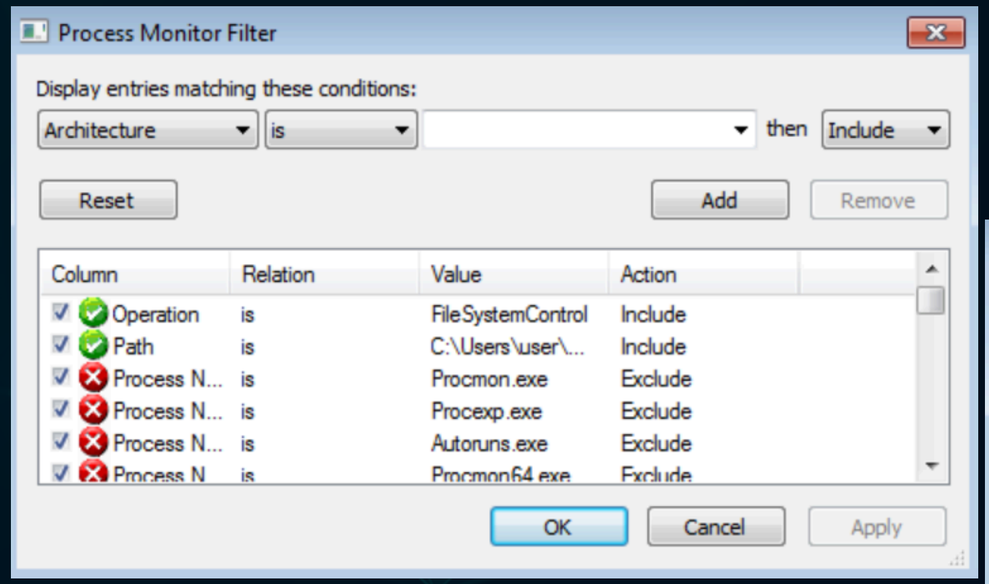


4-Apro ApateDNS ed avvio un server inserendo come DNS il mio IP

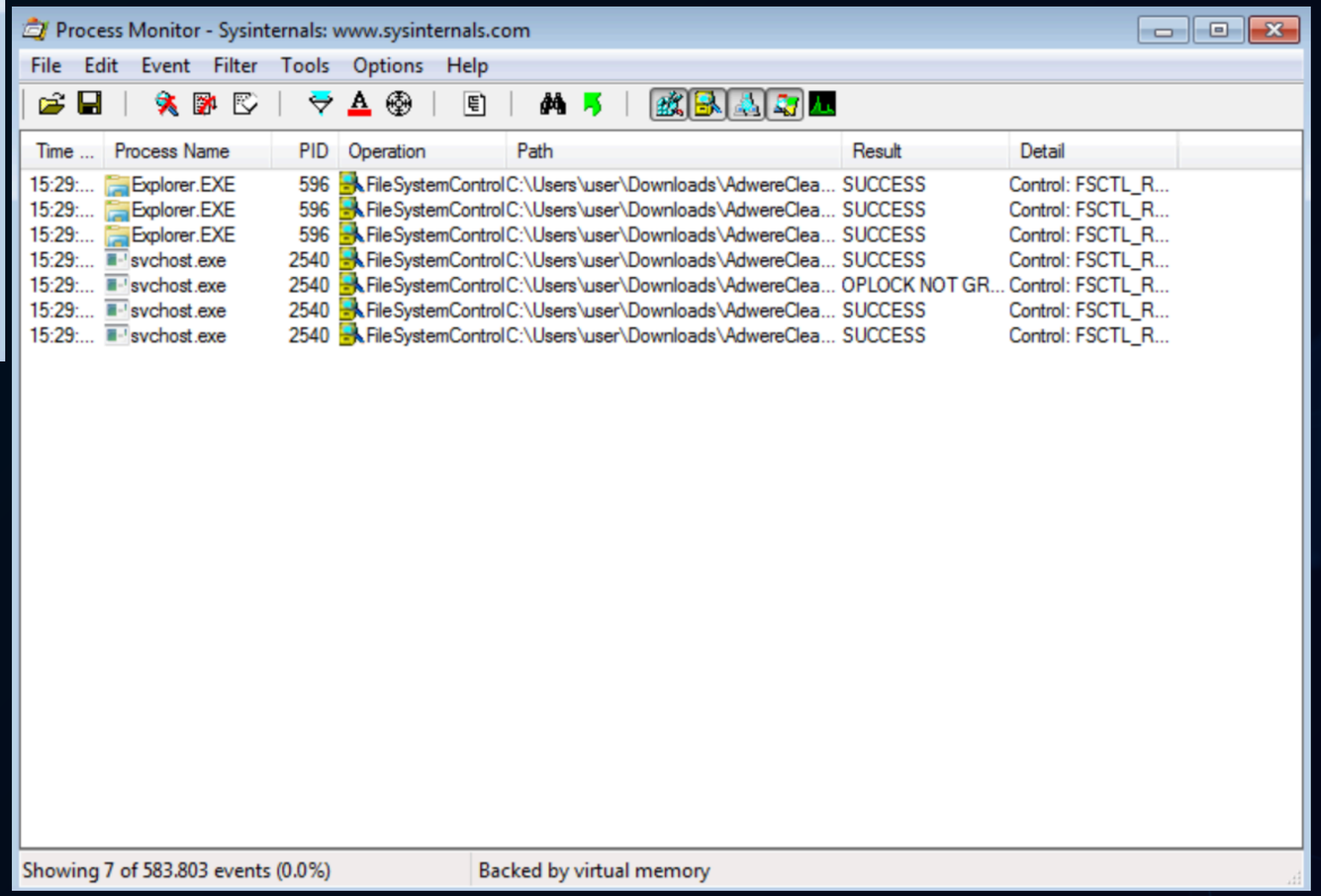


5- Avvio il malware che si presenta come un programma legittimo per rimuovere gli Adw



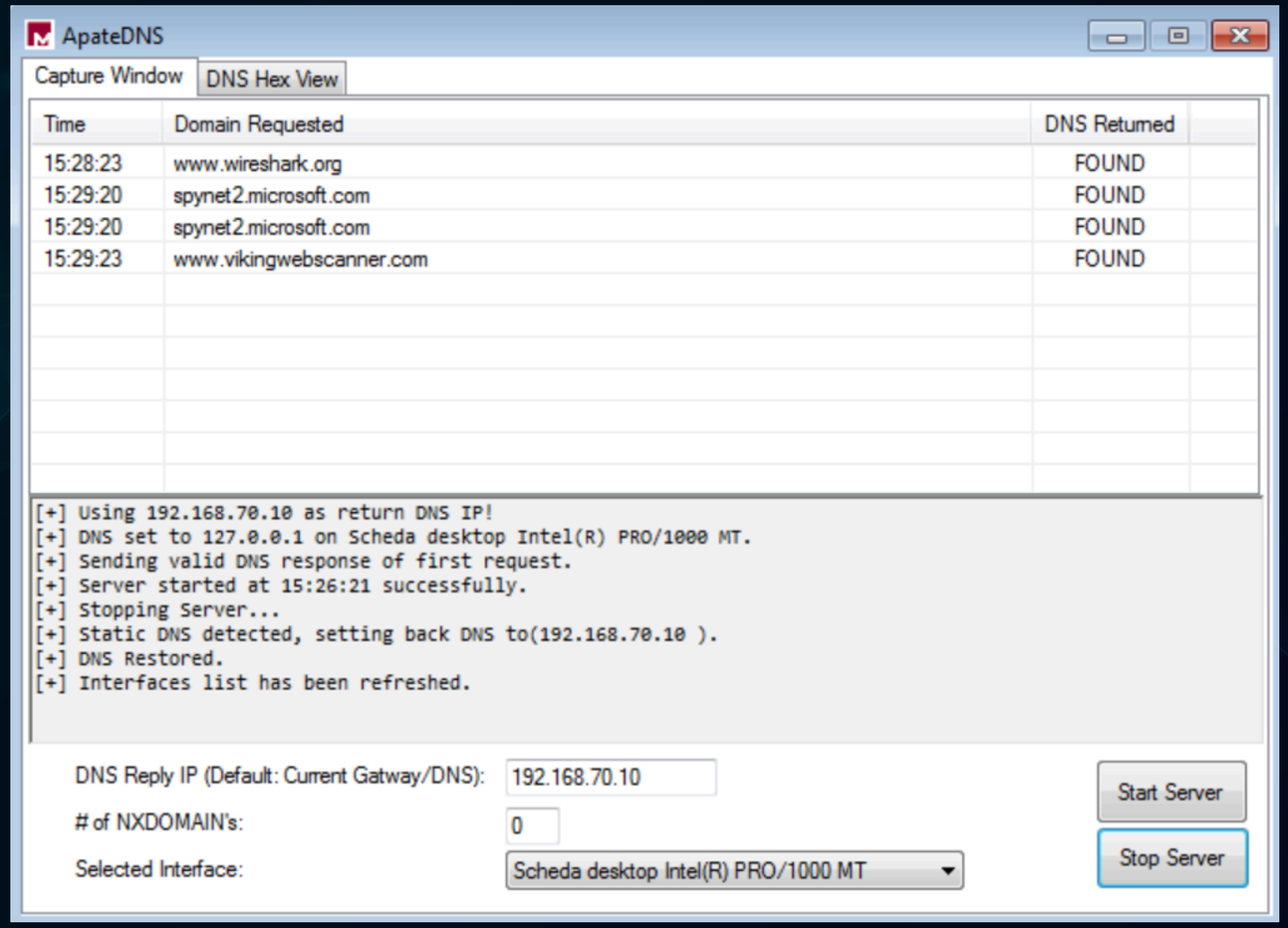


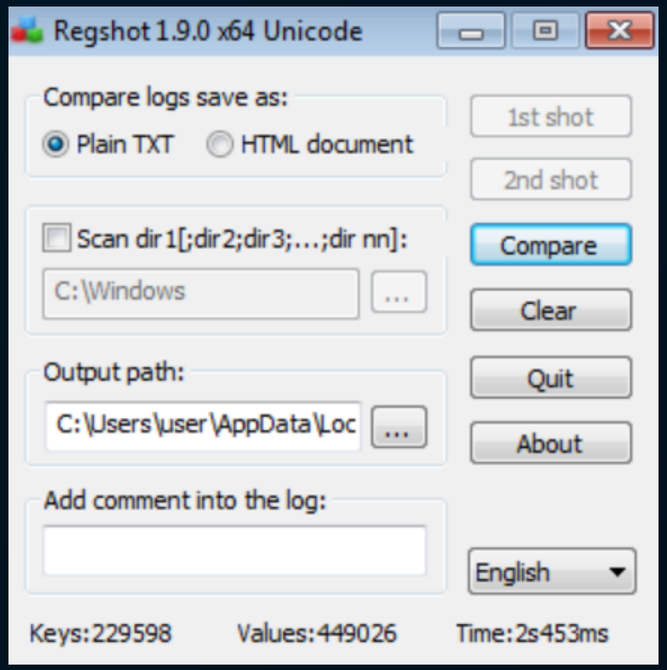
Aggiungo due filtri per filtrare i cambiamenti che mi ha generato il malware, quindi inserisco il path del malware e come tipo di operazione FyleSystem



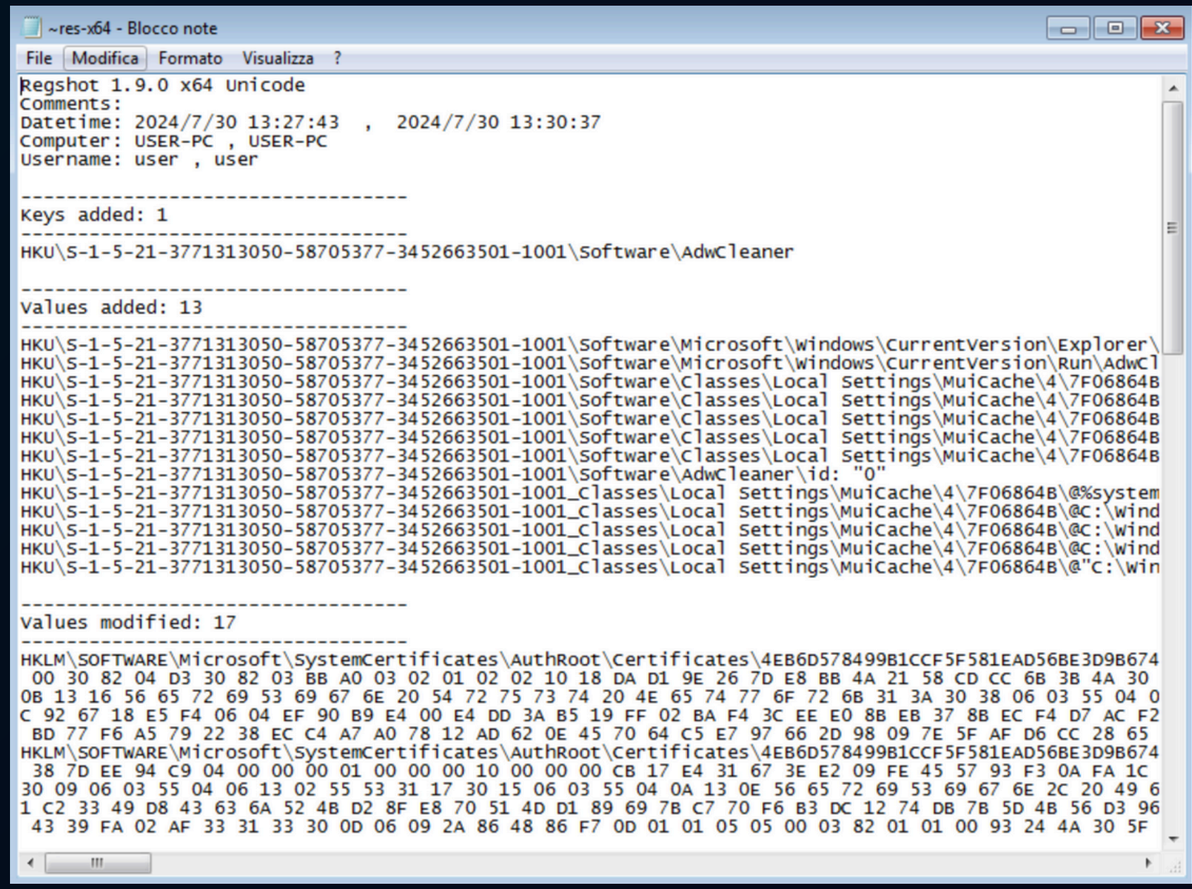
Noto che il malware mi ha cambiato diverse chiavi di registro

Inoltre noto che ha fatto provato a connettersi a domini particolari come vikingwebscanner.com





Faccio la seconda scansione con Regshot e la comparazione con la prima scansione, noto che è stata aggiunta una chiave, 13 valori aggiunti e 17 modificati



In conclusione il malware in questione si spacciava per un altro programma ma in realtà effettuava delle connessioni con domini probabilmente malevoli ed ha cambiato diverse chaivi nel registro per indebolire la protezione