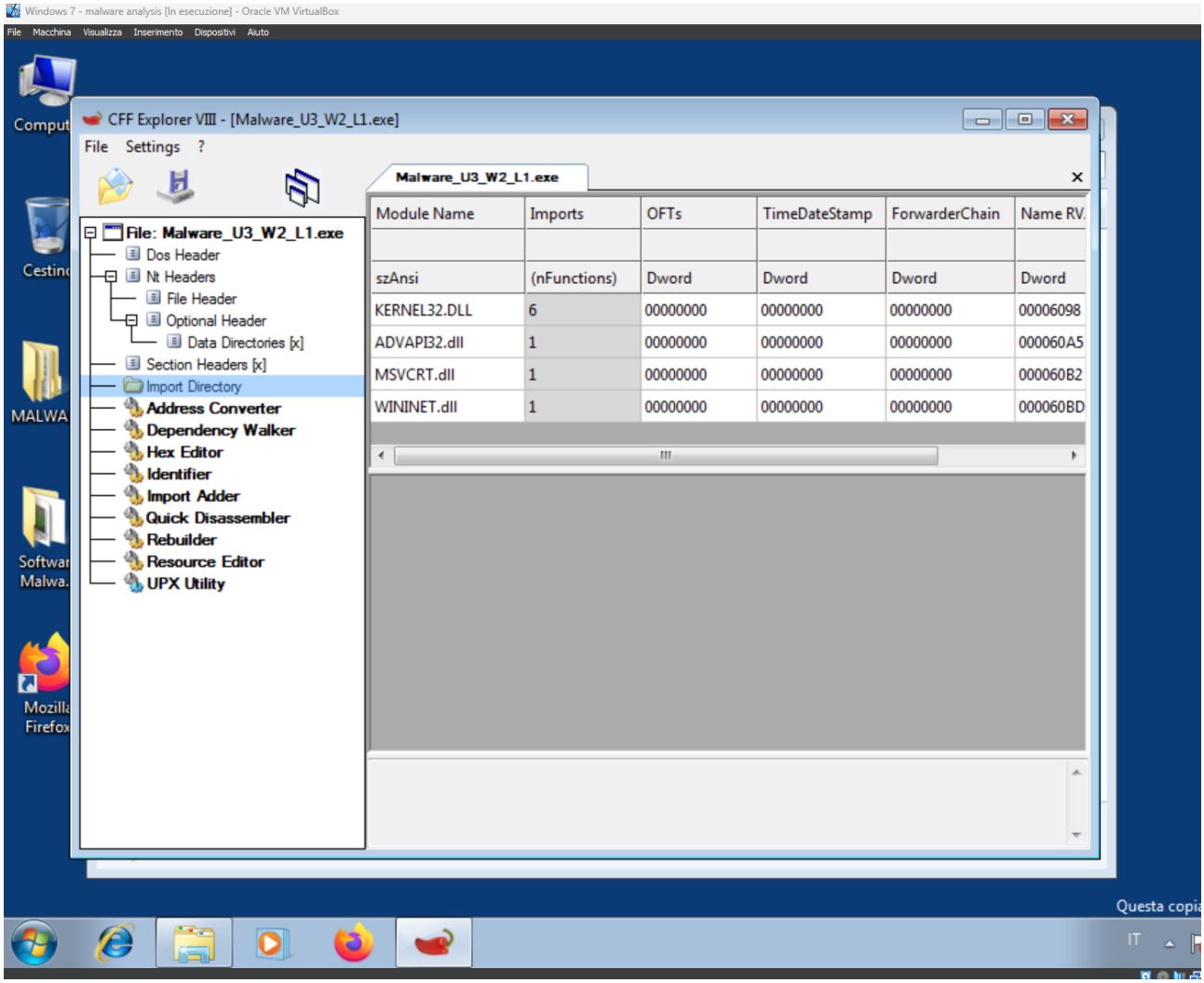
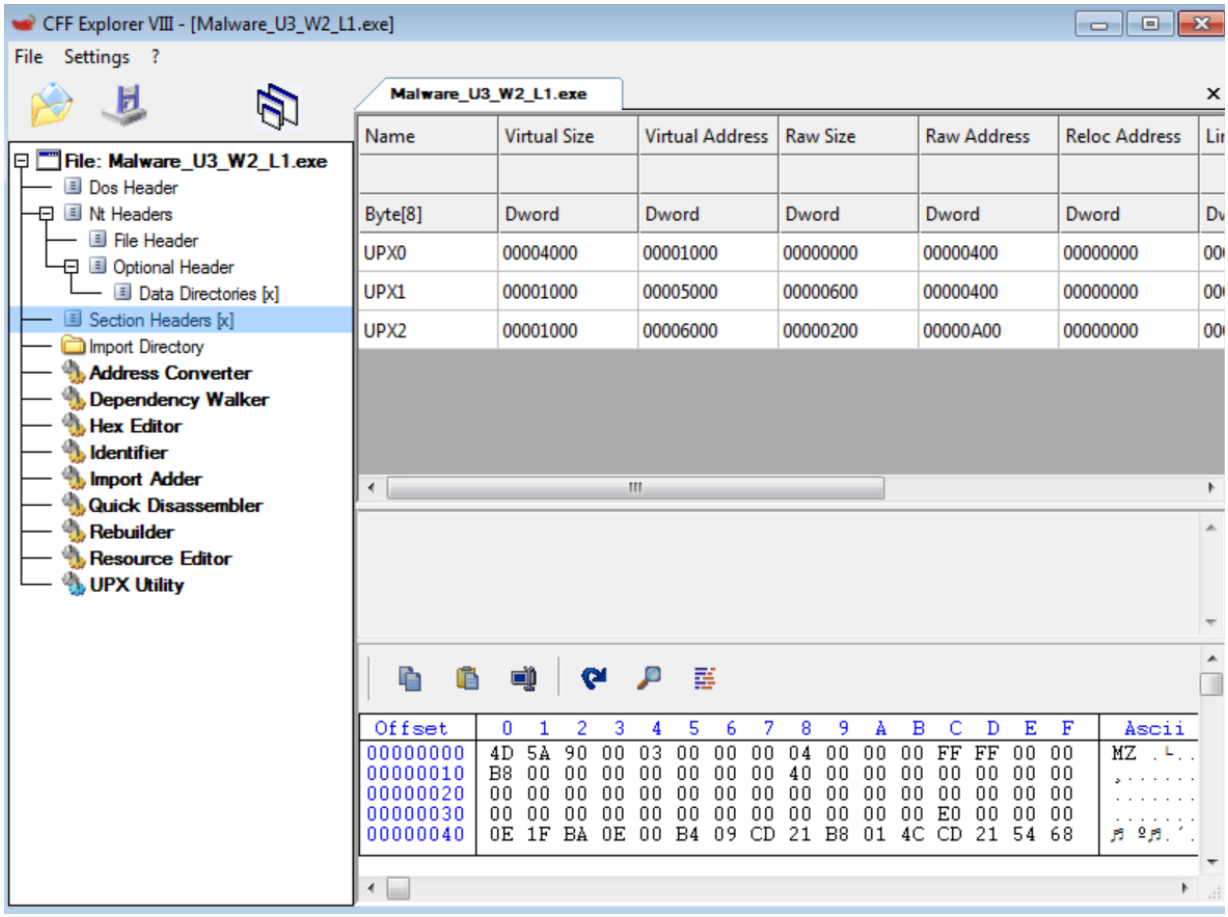
CS2503



Analizzando il malware U3_W2_L1 tramite il software CFF Explorer troviamo 4 sezioni:

- **Kernel32.dll**, che contiene le funzioni principali per interagire con il sistema operativo, ad esempio: manipolazione dei file, la gestione della memoria.
- **Advapi32.dll**, che contiene le funzioni per interagire con i servizi ed i registri del sistema operativo
- **MSVCRT.dll**, che contiene funzioni per la manipolazione stringhe, allocazione memoria e altro come chiamate per input/output, come nel linguaggio C.
- **Wininet.dll che** contiene le funzioni per l'implementazione di alcuni protocolli di rete come HTTP, FTP, NTP.



dalla sezione «section header» vediamo che l'eseguibile si compone di 3 sezioni. Purtroppo sembra che il malware abbia nascosto il vero nome delle sezione.