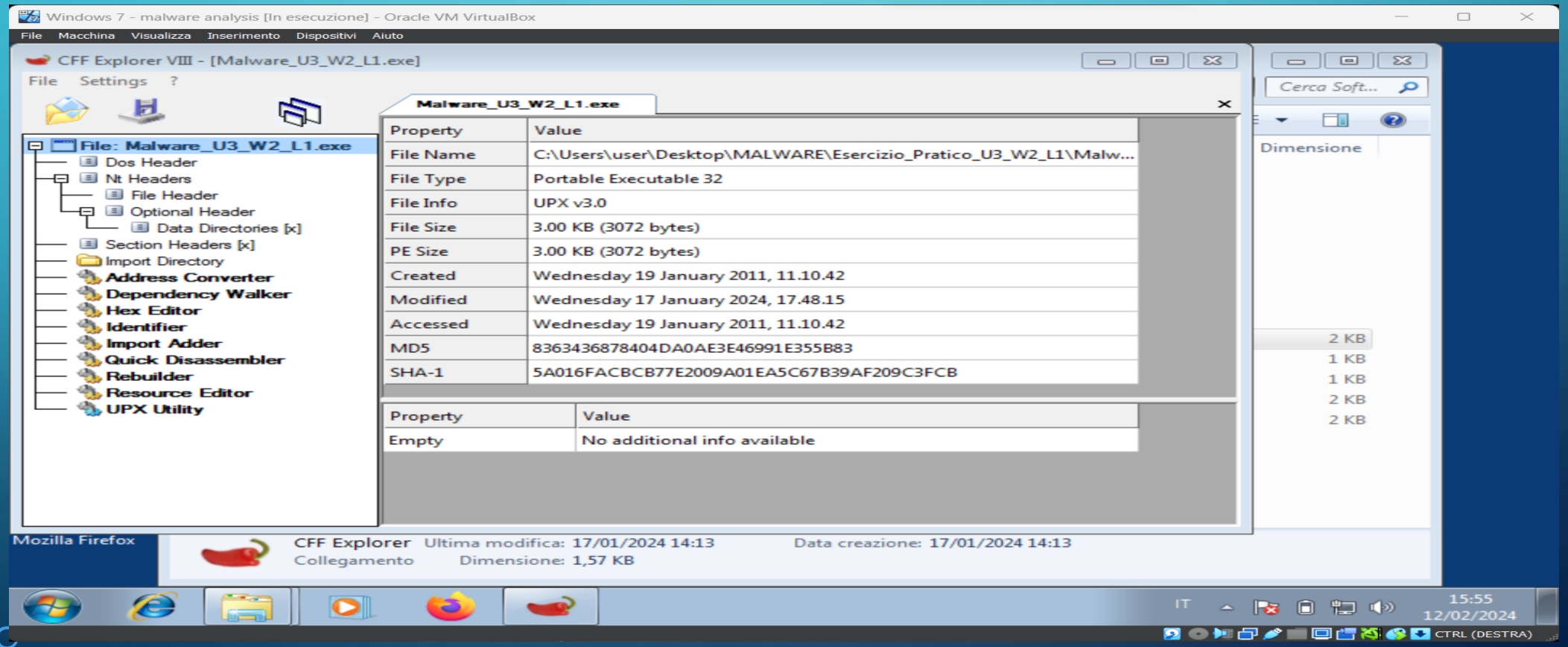
ES LEZIONE 1 SETTIMANA 10

Tramite la nostra macchina virtuale di windows 7 avviamo «CFF Explorer», andiamo ad inserire al suo interno il file «Malware» e andiamo ad analizzarlo.



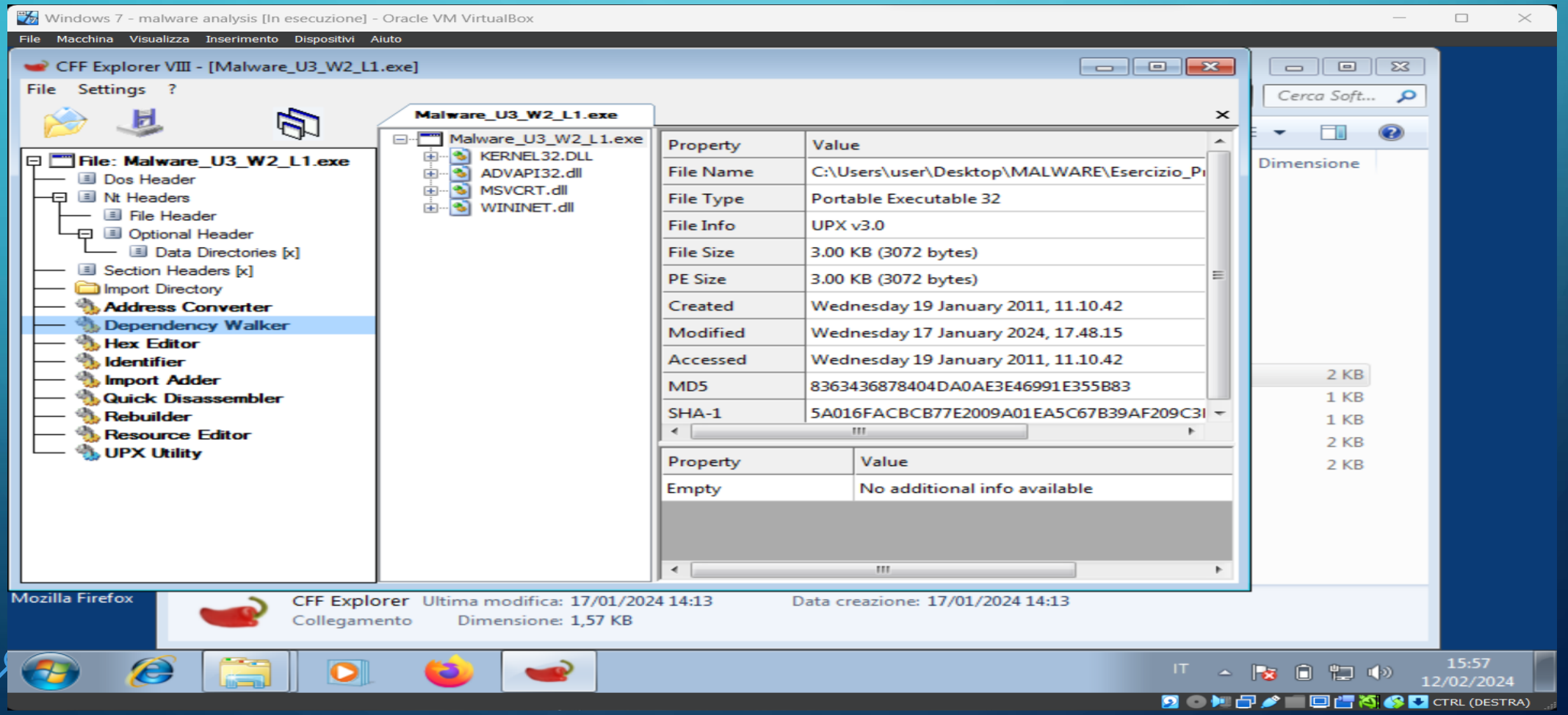
Andiamo ad analizzare le librerie:

° Kernel32.dll: contiene le funzioni principali per interagire con il sistema operativo, ad esempio: manipolazione dei file, la gestione della memoria.

° Advapi32.dll: contiene le funzioni per interagire con i servizi ed i registri del sistema operativo

° MSVCRT.dll: contiene funzioni per la manipolazione stringhe, allocazione memoria e altro come chiamate per input/output, come nel linguaggio C.

° Wininet.dll: contiene le funzioni per l'implementazione di alcuni protocolli di rete come HTTP, FTP, NTP.



Andiamo in fine ad analizzare le sezioni del malware.
Dalle informazioni raccolte possiamo intuire che questo tipo di malware proverà a connettersi alla rete, probabilmente per scaricare nuovo codice malevolo.