Esercizio Forense

Simulazione Esame

DOMANDE

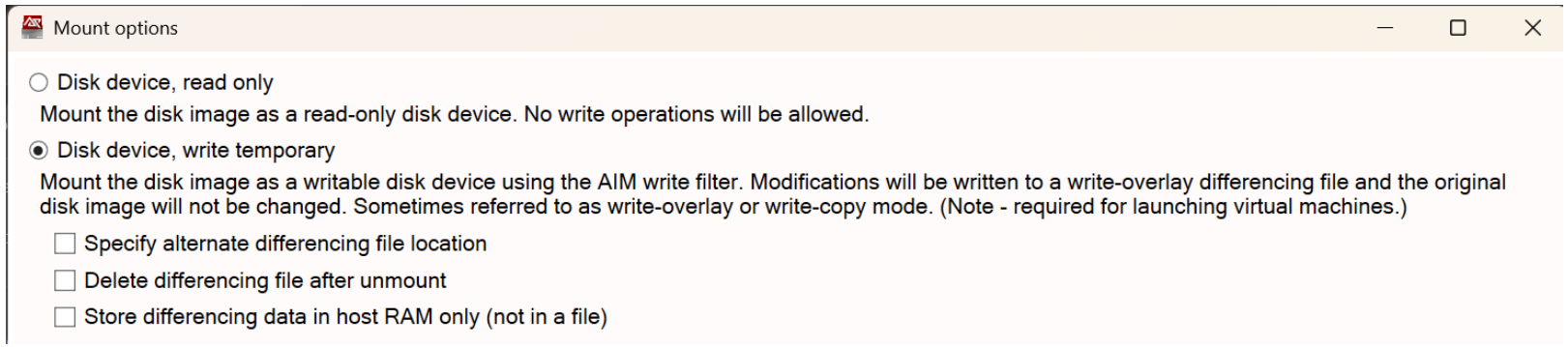
Dato il caso già indicizzato del programma Autospy chiamato PCClient, analizzarlo e rispondere ai seguenti quesiti

1. Quanti utenti ci sono nel PC
2. Qual è l'ultimo utente che ha effettuato l'accesso (Riportare la data)
3. Quale sistema operativo è in esecuzione sul PC e qual è il nome del PC
4. Quando è stato installato il S.O.
5. Sono presenti Client di Posta sul PC
6. Qual è il Timezone in uso sul PC
7. Sono stati installati programmi per catturare il traffico di rete, se si quali
8. Quante volte gli Utenti si sono loggati nel PC
9. Sono presenti email con degli allegati, elencare il nome del mittente e dell'allegato
10. Calcolare l'hash Md5 dei file allegati alle email
11. L'utente scarica l'allegato, dove è stato salvato e cosa contiene
12. Sono presenti connessioni remote al PC
13. Analizzando il PC ci sono dei processi in esecuzione sospetti, elencare quale e tutte le informazioni utili compresi eventuali connessioni.

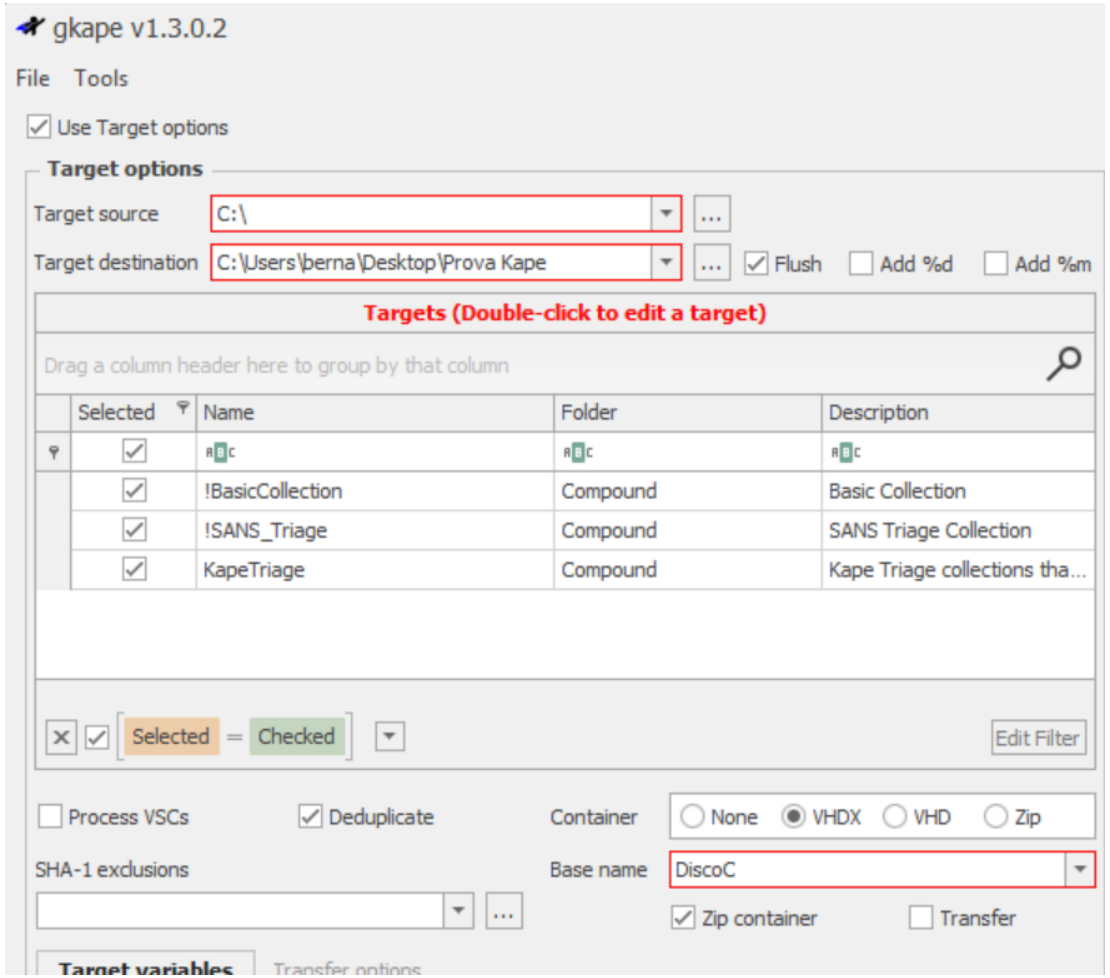
Estrarre la VM denominata PCClient.zip ed importarla in VMWare.

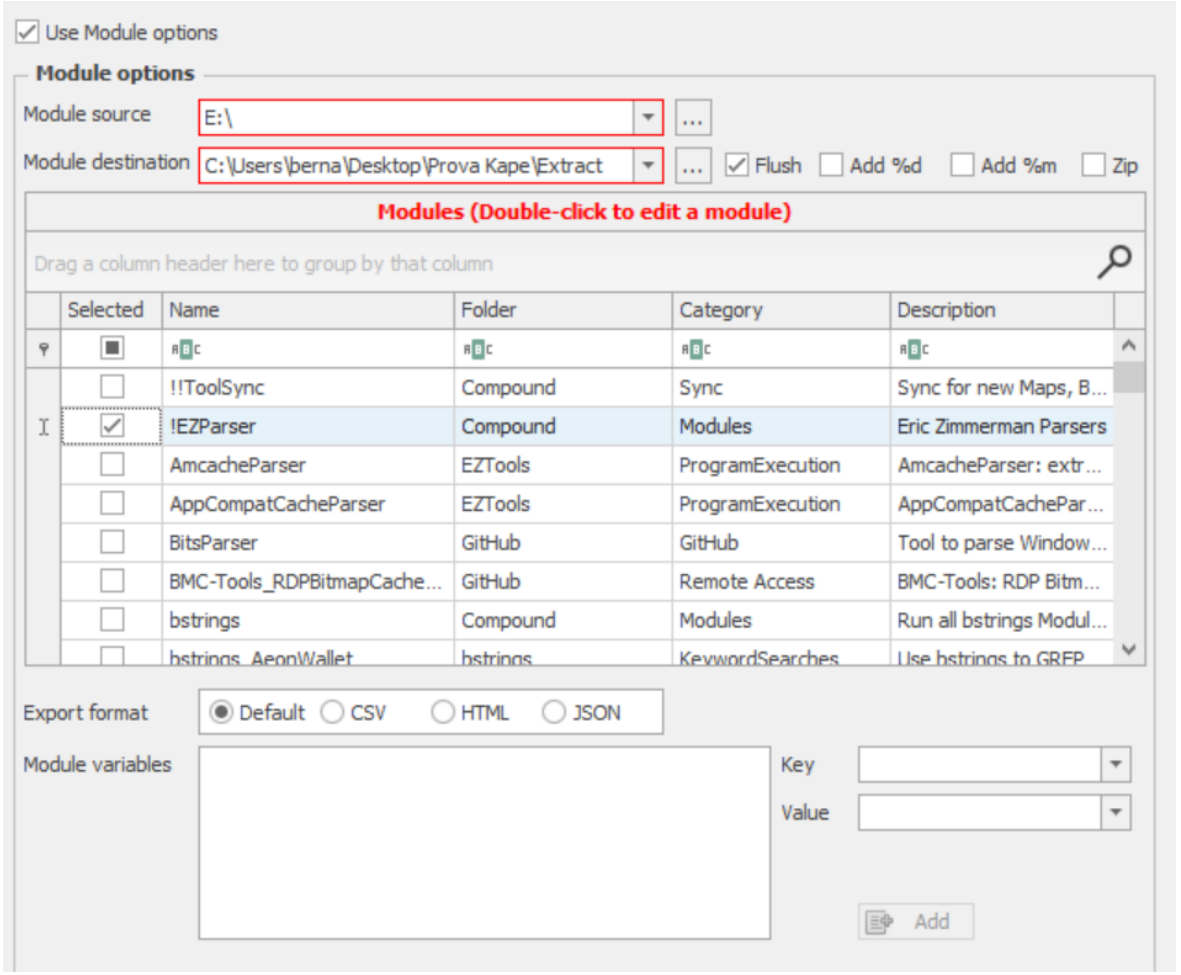
NON ACCENDETELA

Aprite Arsenal Mount Image e caricate il disco che avete importato nella VM e selezione Disk device, Write temporary e cliccate su OK.



Una volta montato il disco, eseguite KAPE (eseguibile gkape) ed eseguite il triage per le analisi, prima la parte TARGET e successivamente la parte dei moduli. Per i Target e i Moduli da eseguire impostate tutto come la foto.

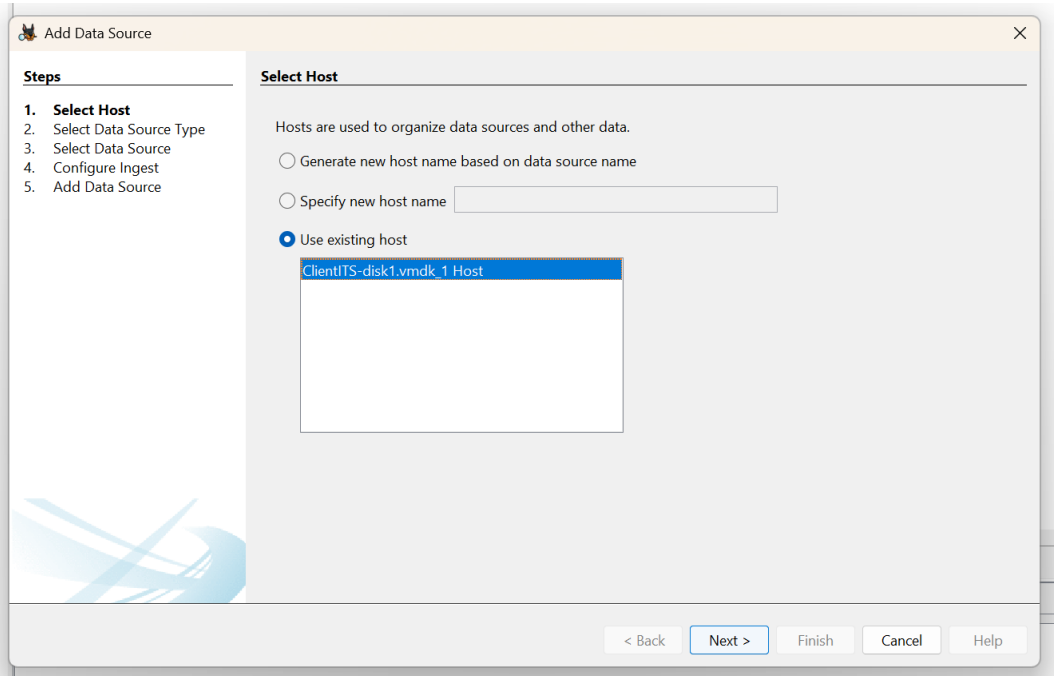


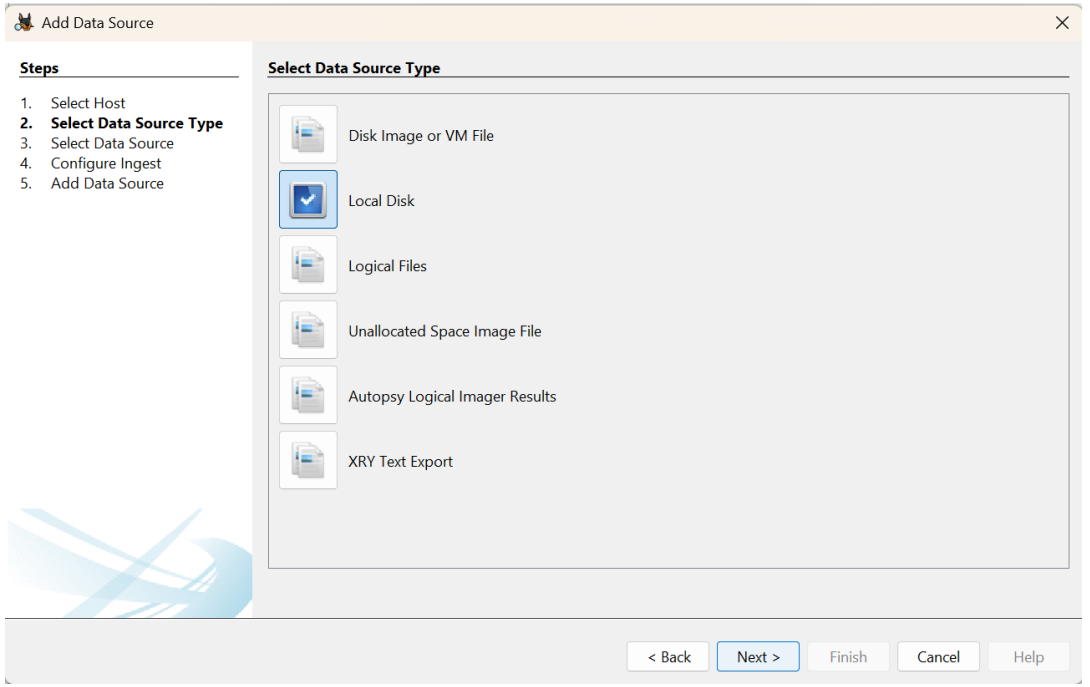


Successivamente create una cartella Autopsy Case ed estraete il contenuto dello zip denominato ClientITS.zip
Aprite Autopsy con "esegui come **Amministratore**" e caricate il caso che è presente nella cartella Autospy Case, vi chiederà la sorgente del disco dati cliccate **NO.**

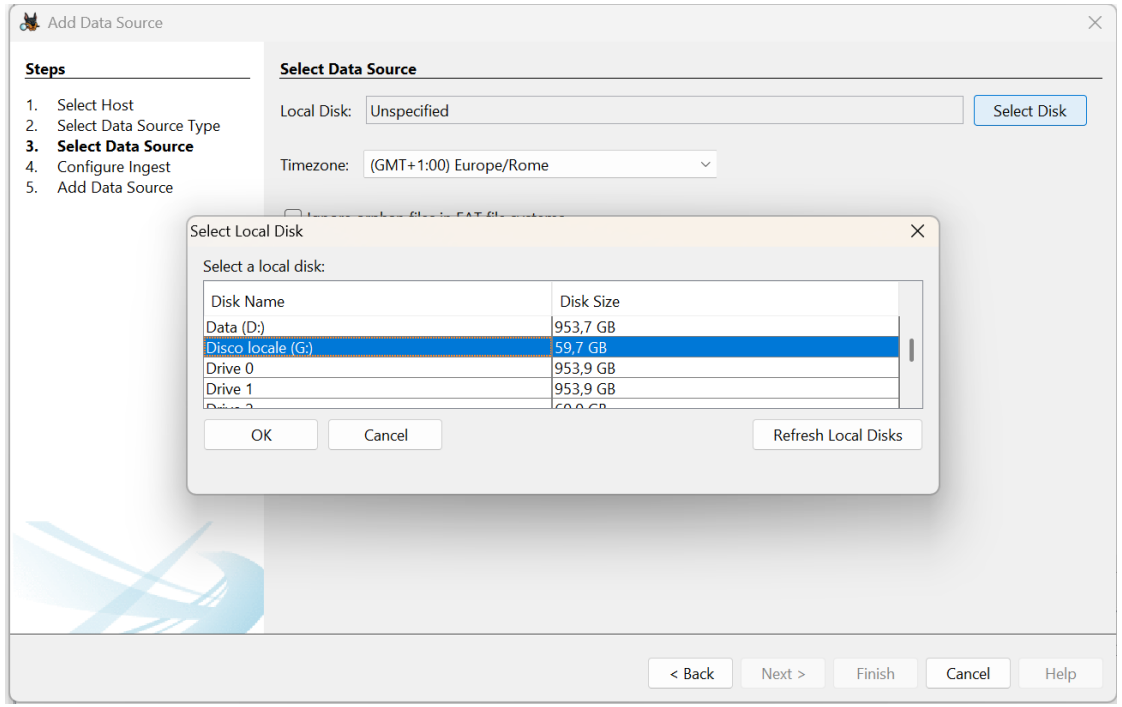
Una volta aperto Autopsy andate in Add Data Source, selezionare Use Existing Host e cliccate l'unico host presente.

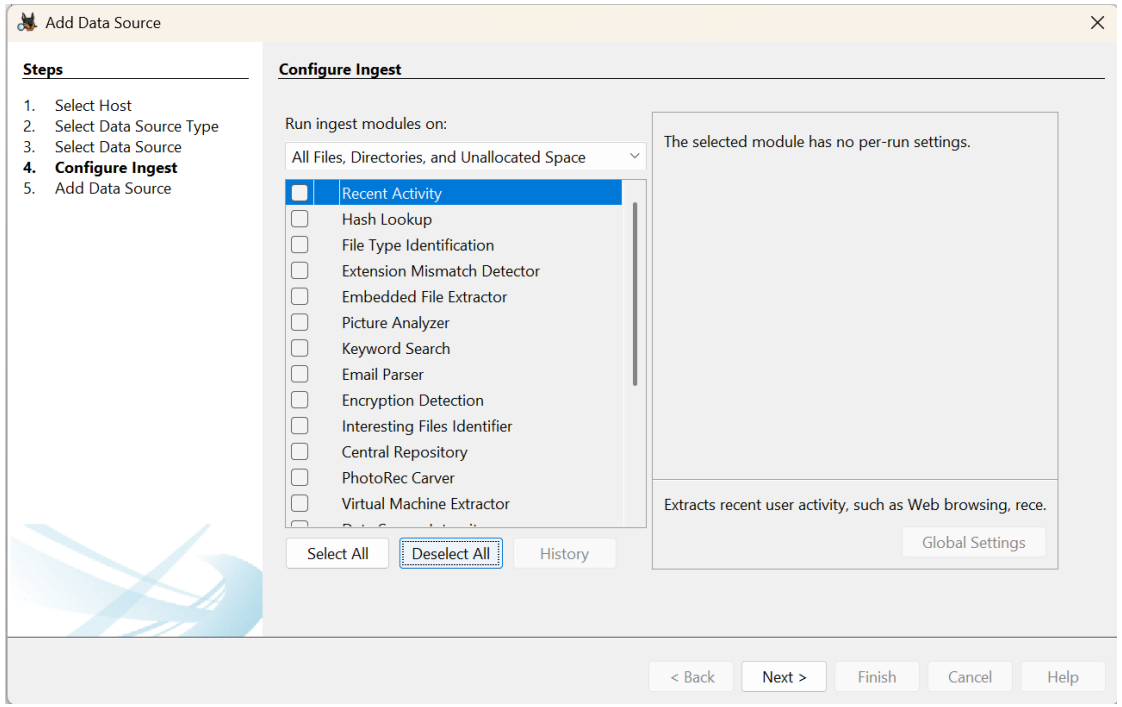
Selezionate come Data Source Local disk e cliccate su Next





Nella schermata successiva cliccate su Local Disk si apre una finestra a tendina e selezione il disco che avete aperto precedentemente con Arsenal Mount Image, nel mio caso G: e cliccate su Next, se non avete aperto Autopsy come Amministratore non vedrete nessun disco.
In configure Ingest cliccate su Deselect All e andate avanti e appena fatto avrete il caso in Autopsy.





Se volete esportare i registri prendeteli nella source G:, i dischi sono uguali soltanto che solo G: permette l'export dei registri di Sistema.