Digital Forensics

Quali sono le fasi della digital forensics?

a. sequestro-catena di custodia - analisi - dibattimento
b. individuazione-acquisizione - analisi - documentazione - presentazione
c. identificazione-preservazione-acquisizione-analisi-documentazione
d. acquisizione - documentazione - analisi – presentazione

La chain of custody è un'attività che si concretizza nelle fasi di:

e. identificazione
f. identificazione e preservazione
g. analisi
h. in tutte le fasi

Se apro un file con il software "MSWord" e lo richiudo senza apportare modifiche il valore della relativa funzione hash:

a. Non cambia
b. Cambia
c. Cambia solo se si usa MD5
d. Cambia solo se si usa SHA1
e. Cambia solo se si esegue il comando "SALVA"

Cos'è un meccanismo write blocker?

a) un dispositivo che, dati un dispositivo sorgente e uno di destinazione, impedisca la scrittura sul dispositivo sorgente
b) qualsiasi sistema software o hardware che, dati un dispositivo sorgente e uno di destinazione, impedisca la scrittura sul dispositivo sorgente
c) un dispositivo che, dati un dispositivo sorgente e uno di destinazione, impedisca la scrittura sul dispositivo destinazione
d) qualsiasi sistema software o hardware che, dati un dispositivo sorgente e uno di destinazione, impedisca la scrittura sul dispositivo destinazione

Quali tra queste problematiche possono verificarsi durante un'analisi "live"?

a) difficoltà nell'eseguire le operazioni
b) perdita del fattore di ripetibilità delle operazioni
c) perdita dei dati post analisi
d) impossibilità di costruire la chain of custody

Come può essere affrontato l'ipotetico problema delle collisioni della funzione di hash?

a) utilizzando 2 differenti funzioni hash contemporaneamente
b) calcolando inizialmente l'hash del dato e successivamente un'ulteriore hash sulla stringa hash già prodotta
c) non è possibile far fronte a questo problema
d) utilizzando una funzione crittografica al posto dell'hash