Digital Forensics – Febbraio 2022

COGNOME:
MATRICOLA:
Email:

- Mobile Forensics: caratteristiche di base (es. ripetibile o non ripetibile), differenze tra acquisizione logica e fisica
- Elencare presupposti e fattispecie tipiche degli accertamenti da eseguirsi in modalità ripetibile e irripetibile
- Elencare le tipiche fasi della Digital Forensics, rapportandole poi ad un possibile caso di studio che coinvolga contenuti multimediali.

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

a. identificazione
b. identificazione e preservazione
c. analisi
d. in tutte le fasi

2) Per la rimozione di rumore "salt&pepper" quale filtro è più indicato:

a. Equalizzare l'istogramma
b. Applicare il filtro mediano
c. Aumentare il contrasto
d. Applicare un filtro media 3x3
e. Applicare un filtro media 5x5
f. Applicare una LUT
g. Applicare un filtro nel dominio della frequenza

3) A cosa è dovuto il problema dell''effetto blocking" su immagini/video?

a. Alla bassa risoluzione
b. Al basso frame rate di acquisizione
c. Al fattore di compressione
d. Al basso contrasto
e. All'Aspect Ratio
f. Al Motion Blur
g. Agli effetti prospettici

4) 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

5) 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

6) In una attività di live forensics in azienda, prima di procedere alle attività di acquisizione, quale tra queste attività va svolta per prima?
a. Fare una privilege escalation
b. Effettuare un de briefing con il cliente e chiedere il supporto di un Amministratore di Sistema
c. Collegare subito un write blocker USB

7) In una attività di live forensics su Windows 10 aggiornato, quale serie di tool dovrà avere il consulente?
a. Password Cracking
b. Chiavetta USB con collezione collaudata di tool live
c. Snort
d. Write blocker

8) Perche, nella digital forensics, sono importanti le modalità di acquisizione e trattamento delle evidenze?
a. Per garantire la ripetibilità delle analisi
b. Per garantire l'autenticità della fonte di prova
c. Per garantire sia l'autenticità della fonte di prova sia la ripetibilità delle analisi
d. Perché si abbiano abbastanza elementi da portare come fonte di prova ai fini legali
e. Tutte le risposte sono corrette

9) La disciplina Multimedia Forensics si occupa di elaborare dati multimediali al fine di procedere con:
a. Identificazione della sorgente di acquisizione e verifica di integrità dei reperti multimediali
b. Analisi, miglioramento, recupero di informazioni semantiche da reperti multimediali
c. Acquisizione, analisi e codifica
d. Recupero targhe e analisi antropometriche
e. Analisi e Miglioramento segnali audio

10) Che ruolo ricopre il Pubblico Ministero nel processo penale
a. Pubblica Accusa
b. Ausiliario dell'avvocato difensore
c. Ausiliario del consulente tecnico di parte
d. Organo giudicante.
e. Giudice a latere
f. Giudice per le indagini preliminare (GIP)
g. Tribunale del Riesame