 

**Digital Forensics – Febbraio 2022**

COGNOME: Raoudi

MATRICOLA: O46001928

Email: Marouanraoudi67@gmail.com

* Mobile Forensics e Disk Forensics: caratteristiche di base e differenze nelle modalità operative di acquisizione e di analisi
* 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.

- la digital forensics è la disciplina che si occupa delle attività d’indagine e consulenze informatiche su dispositivi cellulari utilizzando le tecniche seguente: Identificazione, acquisizione, analisi, valutazione, presentazione.

- Identificazione: Sta nel rilevare cos’è effettivamente utile per l’indagine

* Modalità di acquisizione e certificazione di un contenuto diffamatorio presente sulla piattaforma Facebook

**1) 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

**2) 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

**3) 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

1. **La disciplina Multimedia Forensics si occupa di elaborare dati multimediali al fine di procedere con:**
2. Identificazione della sorgente di acquisizione e verifica di integrità dei reperti multimediali
3. Analisi, miglioramento, recupero di informazioni semantiche da reperti multimediali (Vera)
4. Acquisizione, analisi e codifica
5. Recupero targhe e analisi antropometriche
6. Analisi e Miglioramento segnali audio
7. **L’alibi informatico è :**
8. Non falsificabile
9. Accettato solo quando proviene da log di Social Network (Facebook, Instagram, ecc.)
10. Un altro metodo che negli anni le difese usano per instillare il dubbio che l’accusato non abbia commesso il fatto
11. Una dimostrazione della presenza dell’imputato in un altro luogo rispetto alla esecuzione di un crimine dimostrata in maniera “rigorosa” (Vera)

