Argomentare le seguenti tematiche

[a] Riservatezza dei dati (GDPR)

[b| Descrizione dettagliata delle fasi della Digital Forensics

Domande a risposta multipla

1. La parte civile ...

a. È sempre presente nei processi penali;

b. Coadiuva il giudice di merito per il raggiungimento della verità;

c. Può affiancare il Pubblico Ministero per sostenere l'accusa;

d. Affianca il giudice di legittimità per il raggiungimento della verità.

2. Chi è il consulente tecnico d'ufficio?

a. È un ausiliario del pubblico ministero;

b. È un organo di controllo sull'operato dei giudici;

c. È un organo giurisdizionale di primo grado;

d. È un pubblico ufficiale che può affiancare il giudice nel processo.

3. Cosa vieta il Regolamento europeo sull'intelligenza artificiale, denominato Al Act?

a. Sistemi di polizia predittiva;

b. Sistemi di generazione e manipolazione di contenuti;

c. Sistemi utilizzati come componenti di sicurezza di prodotti;

d. Sistemi destinati all'amministrazione della giustizia.

4. Il secondo comma dell'art. 171 bis della legge sul diritto d'autore punisce chi predispone o utilizza qualsiasi mezzo inteso unicamente a consentire o facilitare la rimozione arbitraria o l'elusione funzionale di dispositivi applicati a protezione di un programma.

a. Si tratta di una fattispecie di illecito amministrativo;

b. Si tratta di una fattispecie di reato di pericolo:

c. Si tratta di una fattispecie criminosa che si perfeziona soltanto se si danneggia il bene protetto;

d. Si tratta di una fattispecie di reato colposo.

5. Cos'è l'informativa per la privacy?

a. È una comunicazione rivolta al titolare del trattamento sulle modalità di svolgimento delle operazioni di trattamento effettuate dall'Autorità Garante;

b. È una comunicazione rivolta all'interessato che ha lo scopo di informarlo sulle finalità e le modalità dei trattamenti operati dal titolare del trattamento;

c. È una comunicazione dell'interessato rivolta al titolare del trattamento per informarlo sui trattamenti lesivi della dignità umana;

d. È una comunicazione dell'interessato rivolta al titolare del trattamento per denunciarlo sulle operazioni di trattamento non consentite dalla legge.

6. 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. Recupero targhe e analisi antropometriche

c. Analisi e Miglioramento segnali audio

d. Analisi, miglioramento, recupero di informazioni semantiche da reperti multimediali

e. Acquisizione, analisi e codifica

7. Qual è la differenza tra image enhancement e image restoration?

a. Image enhancement: Pone a 0 alcuni pixel del segnale originale per migliorarne la qualità. Image restoration: Inverte il processo di degrado del segnale originale.

b. Image enhancement: Inverte il processo di degrado del segnale originale. Image restoration: Migliora la qualità del segnale originale.

c. Image enhancement: Migliora la qualità dell'immagine ripristinandone le caratteristiche originali. Image restoration: Pone a 0 alcuni pixel del segnale originale per invertire il processo di degrado.

d. Image enhancement: Migliora la qualità del segnale originale. Image restoration: Inverte il processo di degrado del segnale sotto esame.

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

a. Identificazione

b. in tutte le fasi

c. analisi

d. identificazione e preservazione

9. Quali delle seguenti affermazioni descrive al meglio le evidenze digitali?

a. Le evidenze digitali sono duplicabili.

b. Le evidenze digitali sono volatili ed inalterabili

c. Le evidenze digitali rappresentano sempre dei fatti probatori durante l'iter

d. Le evidenze digitali sono volatili. duplicabili e alterabili

10. 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 destinazione

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

d. un dispositivo che dati un dispositivo sorgente e uno di destinazione, impedisca la scrittura sul dispositivo destinazione

11. Elencare in ordine decrescente di sicurezza le seguenti funzioni HASH:

a. Md-5, SHA-256, SHA-512

b. SHA-512, MD5, SHA-256

c. SHA-512, SHA-256, MD-5

d. SHA-256. SHA-512, MD-5

12. 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

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

a. utilizzando 2 differenti funzioni hash contemporancamente

b. utilizzando la una funzione crittografica al posto dell'hash

c. calcolando inizialmente l'hash del dato e successivamente un'ulteriore hash sulla stringa hash già prodotta

d. non è possibile far fronte a questo problema

14. I software di wiping riescono a cancellare anche i dati presenti nello "Slack Space"

a. Si

b. Dipende dalle configurazioni di sistema e dai relativi protocolli di sicurezza

c. In parte

d. No

15. Presupposti reato di Diffamazione in Rete

a. Presenza di messaggi privati lesivi della reputazione su piattaforme di messagistica

b. Comunicazione a mezzo social network con contenuti diffamatori

c. Assenza dell'offeso, Offesa all'altrui reputazione, Comunicazione a più persone

16. 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. Collegare subito un write blocker USB

c. Effettuare un debriefing con il cliente e chiedere il supporto di un Amministratore di Sistema

17. Quali sono le fasi della digital forensics?

a. individuazione-acquisizione - analisi - documentazione - presentazione

b. sequestro-catena di custodia - analisi - dibattimento

c. acquisizione - documentazione - analisi – presentazione

d. identificazione-preservazione-acquisizione-analisi-documentazione

18. La nomina del CTP nei procedimenti giudiziari avviene a cura

a. dagli Ufficiali di Polizia Giudiziaria

b. del legale o direttamente dalla parte, dal Pubblico Ministero

c. del cancelliere del Tribunale

d. dal Giudice

19. Valore legale messaggio di Posta Elettronica

a. Documento Informatico

b. Nessuna validità a seguito della impossibilità di garantire l'integrità, la paternità e altre caratteristiche correlate.

c. Documento informatico sottoscritto con firma digitale

d. Documento informatico sottoscritto con firma semplice

20. Quali tra i seguenti programmi può essere utilizzato per effettuare una copia forense:

a. Foremost

b. Guymager

c. MemDump

d. Imount

e. Hashdb

f. mount-nfs

21. Cos'è la perquisizione informatica?

a. Uso di dettagliate tecniche forense per l'estrazione e l'analisi di dati presenti negli hard disk

b. Metodologie forensi per il sequestro di dispositivi informatici

c. Mezzo di ricerca delle prove sui contenuti di sistemi informatici

d. Tecniche di estrazione, analisi e miglioramento dei contenuti multimediali per la risoluzione di un caso per l'identificazione di prove univoche

22. Legge n°48 del 18 marzo 2008

a. Sancisce i principi fondanti della computer forensics all'interno del nostro ordinamento

b. Si riferisce ad accertamenti tecnici ripetibili

c. Definisce i principi base dei Bias Cognitivi in ambito forense sulle immagini

d. Definisce la figura professionale del Digital Forensic Expert

23. Caratteristiche PEC:

a. Integrità del Messaggio, Certificazione dell'invio, Certificazione della Consegna

b. Integrità degli Allegati, Certificazione dell'Invio, Certificazione del Destinatario

c. Integrità del Messaggio, Certificazione del Mittente, Certificazione della Consegna

d. Integrità degli Allegati, Certificazione del Mittente, Certificazione della Consegna

24. Perché, nella digital forensics, sono importanti le modalità di acquisizione e trattamento delle evidenze?

a. Per garantire la ripetibilità delle analisi

b. Perché si abbiano abbastanza elementi da portare come fonte di prova ai fini legali

c. Per garantire l'autenticità della fonte di prova

d. Tutte le risposte sono corrette

e. Per garantire sia l'autenticità della fonte di prova sia la ripetibilità delle analisi

1) Che tipo di iter normativo seguirà il disegno di legge sull'intelligenza artificiale in Italia?

a. Sarà discusso dal Parlamento e sarà emanato dal Governo.

b. È già stato approvato dal Parlamento e sarà promulgato sotto forma di decreto-legge.

c. È proposto dal Governo e dovrà essere approvato dal Parlamento.

d. È proposto dall'Unione europea e sarà promulgato dal Capo dello Stato.

2) Cosa prevede il disegno di legge sull'intelligenza artificiale a proposito di professioni intellettuali?

a. Esso pone alcuni limiti all'impiego dell'IA: non potrà essere utilizzata dal prestatore d'opera se impatta con la vita privata del committente.

b. Esso pone alcuni limiti all'impiego dell'IA: se il prestatore d'opera li utilizza dovrà calcolare uno sconto in fattura.

c. Esso non pone limiti all'impiego dell'IA: potrà essere utilizzata dal prestatore d'opera a prescindere dal consenso del committente.

d. Esso pone alcuni limiti all'impiego dell'IA: potrà essere utilizzata solo per attività strumentali e di supporto alla prestazione e prevede che la parte umana abbia un apporto prevalente.

3) Ai sensi del disegno di legge sull'intelligenza artificiale in Italia, come potranno essere utilizzati i sistemi di IA nell'ambito dell'attività giudiziaria?

a. Potranno essere assunte decisioni dai sistemi di IA purché adeguatamente motivate.

b. Potranno essere assunte decisioni dai sistemi di IA purché non prevedano misure detentive.

c. I sistemi di IA potranno essere utilizzati esclusivamente per l'organizzazione e la semplificazione del lavoro giudiziario, riservando al magistrato ogni decisione.

d. I sistemi di IA potranno essere utilizzati esclusivamente per la semplificazione del sistema giustizia, ivi comprese le determinazioni di tipo predittivo.

4) In applicazione di Image/Video Forensics, qual è l'effetto dell'applicazione della media tra pixel corrispondenti su diversi frame di una sequenza di immagini disturbate da rumore casuale a media nulla? Considerando anche di applicato un'operazione di Image Registration.

a. Il rumore casuale viene completamente eliminato anche con un numero ridotto di fotogrammi.

b. L'effetto della media tra i pixel dei diversi frame è insignificante sulla riduzione del rumore.

c. La media tra i pixel dei diversi frame riduce il rumore, ma solo con un numero infinito di fotogrammi.

d. Anche con un numero ridotto di fotogrammi, la media tra i pixel dei diversi frame può produrre risultati notevoli nella riduzione del rumore.

5) Cosa si intende per FNU (Fixed Pattern Noise)?

a. La combinazione non uniforme di tutte le imperfezioni che caratterizzano il dispositivo di acquisizione (come smartphone)

b. Il rumore definito dalle stime dei pixel ottenute dalle operazioni di interpolazione dopo l'applicazione del pattern CFA nelle macchine fotografiche

c. È definito come le differenze da pixel a pixel quando l'array di sensori non è esposto alla luce.

d. La sensibilità dei pixel alle ombre rimosse dalla blocchettatura nel processo di compressione JPEG.

6) Per la rimozione di rumore periodico quale filtro è più indicato:

a. Applicare il filtro mediano

b. Applicare un filtro media 3x3

c. Applicare un filtro media 5x5

d. Applicare un filtro nel dominio della frequenza

e. Equalizzare l'istogramma

f. Aumentare il contrasto

g. Applicare una LUT

7) Cosa si intende per Photoshop Forensic?

a. Applicazioni di tecniche di Image Processing per migliorare la qualità dei dati digitali ed estrarre le evidenze desiderate

b. Tutte quelle tecniche in grado di falsificare digitalmente contenuti multimediali di qualsiasi natura

c. L'uso di Photoshop per migliorare la qualità dei dati digitali ed estrarre le evidenze desiderate

d. Tecniche forensi atte ad analizzare dati digitali attraverso approcci "Photoshop" (applicazioni di filtri, ecc..) al fine di definire l'autenticità e l'integrità.

8) Watermark Fragile e Semi-Fragile:

a. Watermark Fragile: sono meno sensibili alle modifiche dei pixel. Watermark Semi-Fragile: sono progettate per rilevare ogni possibile cambiamento nei valori dei pixel.

b. Watermark Fragile: sono progettate per rilevare ogni possibile cambiamento nei valori dei pixel. Watermark Semi-Fragile: sono meno sensibili alle modifiche dei pixel.

c. Watermark Fragile: sono difficili da rilevare e risultano essere robusti alla compressione JPEG. Watermark Semi-Fragile: le informazioni sono nascoste tra il dominio spaziale e il dominio frequenziale, sono difficili da rilevare e un attacco di compressione JPEG può distruggere in modo parziale l'informazione

d. Watermark Fragile: sono facili da rilevare e risultano essere robusti alla compressione JPEG. Watermark Semi-Fragile: le informazioni sono nascoste solo nel dominio frequenziale e risultano essere robusti alla compressione JPEG.

9) Quali elementi definiscono il comportamento dei kernel nei filtri convolutivi?

a. I valori dei pixel nell'immagine

b. I valori dei pesi della maschera convolutiva

c. La funzione applicata a ciascun pixel

d. L'intorno del pixel

10) Le immagini affette da Motion Blur possono essere migliorate

a. Mai

b. Solo in particolari condizioni legate alla tipologia di moto presente nella scena

c. Solo attraverso l'utilizzo di particolari filtri di deconvoluzione

d. Solo in presenza di rumore periodico

e. Sempre

11) Come è possibile comprimere un video?

a. Utilizzando solo tecniche lossless per garantire la reversibilità della compressione.

b. Utilizzando solo tecniche lossy per ottenere una maggiore compressione.

c. Sfruttando le caratteristiche intrinseche del video stesso e le caratteristiche del sistema visivo umano.

d. Eliminando completamente le informazioni ritenute "sacrificabili" senza considerare le caratteristiche del sistema visivo umano.

12) Qual è il metodo utilizzato per riconoscere il movimento in un sistema di videosorveglianza?

a. La tecnica di foreground subtraction, che sottrae il background da ogni fotogramma per individuare le differenze.

b. L'utilizzo di sensori di movimento posizionati nelle aree monitorate per rilevare cambiamenti.

c. Il calcolo della media dei valori dei pixel in un fotogramma per determinare la presenza di movimento.

d. L'analisi delle informazioni audio associate ai fotogrammi per riconoscere il suono del movimento.

13) Nelle immagini JPEG, dove devono essere applicate le tecniche di steganografia per nascondere l'informazione desiderata?

a. Nel canale della luminanza

b. Nei canali della crominanza

c. Nei coefficienti di Fourier

d. Nel processo di quantizzazione

14) Secondo le linee guida riportate nel documento ENFSI-BPM, quali sono le incoerenze ottiche che possono essere presenti su un'immagine?

a. Incoerenze dovute dalla luce e da definiti punti di riferimento

b. ombre, presenza di oggetti trasparenti, presenza di oggetti riflettenti e sfocatura

c. ombre, presenza di specchi nella scena, artefatti prodotti dalla compressione JPEG

d. Presenza di oggetti trasparenti e presenza di oggetti riflettenti

15) Mobile Foreniscs - acquisizione della RAM

a. Deve necessariamente essere effettuata in ogni dispositivo

b. Occorre prima riavviare il dispositivo e successivamente, accedere come root e procedere ad effettuare l'acquisizione.

c. Può essere effettuata solo tramite root

d. Viene fatta raramente e non necessariamente serve accedere come root