1) In una attività di live forensics in azienda, prima di procedere alle attività di acquisizione, quale tra queste attività va svolta per prima?

- Fare una privilege escalation
- Effettuare un de briefing con il cliente e chiedere il supporto di un Amministratore di Sistema
- 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?

- Password Cracking
- Chiavetta USB con collezione collaudata di tool live
- Snort
- Write blocker

3) Perche, nella digital forensics, sono importanti le modalità di acquisizione e trattamento delle evidenze?

- Per garantire la ripetibilità delle analisi
- Per garantire l'autenticità della fonte di prova
- Per garantire sia l'autenticità della fonte di prova sia la ripetibilità delle analisi
- Perché si abbiano abbastanza elementi da portare come fonte di prova ai fini legali
- Tutte le risposte sono corrette

4) La disciplina Multimedia Forensics si occupa di elaborare dati multimediali al fine di procedere con:

- Identificazione della sorgente di acquisizione e verifica di integrità dei reperti multimediali
- Analisi, miglioramento, recupero di informazioni semantiche da reperti multimediali
- Acquisizione, analisi e codifica
- Recupero targhe e analisi antropometriche
- Analisi e Miglioramento segnali audio

5) L'alibi informatico è :

- Non falsificabile
- Accettato solo quando proviene da log di Social Network (Facebook, Instagram, ecc.)
- Un altro metodo che negli anni le difese usano per instillare il dubbio che l'accusato non abbia commesso il fatto
- Una dimostrazione della presenza dell'imputato in un altro luogo rispetto alla esecuzione di un crimine dimostrata in maniera "rigorosa"

6) Che ruolo ricopre il Pubblico Ministero nel processo penale

- Pubblica Accusa
- Ausiliario dell'avvocato difensore
- Ausiliario del consulente tecnico di parte
- Organo giudicante.
- Giudice a latere
- Giudice per le indagini preliminare
- Tribunale del Riesame

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

- identificazione
- identificazione e preservazione
- analisi
- in tutte le fasi

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

- Equalizzare l'istogramma
- Applicare il filtro mediano
- Aumentare il contrasto
- Applicare un filtro media 3x3
- Applicare un filtro media 5x5
- Applicare una LUT
- Applicare un filtro nel dominio della frequenza

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

- Alla bassa risoluzione
- Al basso frame rate di acquisizione
- Al fattore di compressione
- Al basso contrasto
- All'Aspect Ratio
- Al Motion Blur
- Agli effetti prospettici

10) Cos'è un meccanismo write blocker?

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

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

- difficoltà nell'eseguire le operazioni
- perdita del fattore di ripetibilità delle operazioni
- perdita dei dati post analisi
- impossibilità di costruire la chain of custody
-

12) Quali sono le fasi della digital forensics?

- sequestro-catena di custodia - analisi - dibattimento
- individuazione-acquisizione - analisi - documentazione - presentazione
- identificazione-preservazione-acquisizione-analisi-documentazione
- acquisizione - documentazione - analisi – presentazione

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

- Non cambia
- Cambia
- Cambia solo se si usa MD5
- Cambia solo se si usa SHA1
- Cambia solo se si esegue il comando "SALVA"

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

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

15) Quale tra i seguenti elementi se presenti può essere utilizzato per garantire l'autenticità e l'esistenza di un messaggio di posta elettronica?

- La presenza e il relativo valore del campo DKIM
- La presenza e il relativo valore del campo Message_ID
- La ricevuta di ritorno
- La presenza nell'header di un indirizzo IP valido e di un indirizzo mail del mittente valido

16) il c.p.p. all'art. 359 si riferisce ad accertamenti tecnici ripetibili. Se si sta operando in regime di art. 359, è possibile:

- Non effettuare il calcolo dell'hash del dato digitale
- Non effettuare la cifratura del dato digitale
- Utilizzare software open source
- Effettuare operazioni senza la presenza della controparte

17) Nell'acquisizione sistema di video sorveglianza su DVR è consigliabile:

- Esportare i dati nel formato proprietario
- Procedere al sequestro del DVR ed eseguire una copia forense del disco
- Visualizzare e salvare in JPEG solo i fotogrammi di interesse
- Esportare i dati in formato JPEG
- Esportare i dati in formati standard AVI, MP4, ecc

18) Quali delle seguenti affermazioni rispetto all'analisi forense di un file multimediale acquisito da uno smartphone e condiviso su Facebook (senza applicazione di filtri e/o di editing) è vera:

- Il file non è integro ma autentico
-

19) Il c.p.p. all'art. 360 si riferisce ad accertamenti tecnici non ripetibili, in quali fasi della digital forensics può presentarsi?

- In tutte le fasi

20) Se apro un file con un semplice editor di testo / software di editing e lo richiudo senza apportare modifiche, il valore della relativa funzione hash:

- Cambia
- Non cambia
- Altro
- Cambia solo se usiamo MD5
- Cambia solo se usiamo SHA1

21) Per la rimozione del rumore impulsivo quale filtro è più indicato?

- Equalizzare l'istogramma
- Applicare il filtro mediano
- Aumentare il contrasto
- Applicare il filtro media 3x3
- Applicare una LUT
- Applicare un filtro nel dominio delle frequenze

22) Nel GPDR quali dei seguenti dati personali possono essere trattati solo in particolari casi e con una speciale attenzione e prudenza?

- I dati anagrafici
- I dati anonimi
- I dati relativi allo stato di salute
- I dati delle imprese private

23) Cosa indica il principio della privacy by design inserito nel regolamento europeo?

- La necessità di proteggere i sistemi fin dalla progettazione

24) I software di wiping riescono a cancellare anche i dati presenti nello Slack Sace?

- Si
- No
- In Parte
- Altro

25) Funzioni hash per il calcolo dell'integrità di un file

- SHA-256, MD5
- JPEG, MPEG
- MP3, AAC, Wave
- RSA
- ISO90100

26) L'immagine acquisita da uno smartphone e immediatamente condivisa su un canale social è

- Autentica
- Integra
- Altro

27) Il problema delle collisioni nell'utilizzo di funzioni hash è:

- Gestibile attraverso un'opportuna memoria tecnica da accludere nella consulenza
- Gestibile attraverso procedure opportune da considerare caso per caso
- Gestibile attraverso l'utilizzo di due funzioni hash differenti
- Trascurabile in applicazioni pratiche

28) Il reato di diffamazione in Rete è perseguibile solo se:

- Ve ne siano i presupposti giuridici previsti
- Avviene a mezzo stampa
- Viene certificato ed acquisito correttamente l'ID

29) In cosa consiste l'acquisizione tramite duplicazione/clone?

- Creare una copia 1:1 del dispositivo sorgente su un supporto equivalente
- Creare una copia immagine del dispositivo sorgente

30) Best practice per l'acquisizione di una pagina web?

- Acquisizione traffico di rete ecc
- Stampa della pagina in PDF
- Stampa della pagina
- Utilizzo di software proprietari

31) Caratteristiche del reperto informatico

- Volatile, Alterabile, Duplicabile
- Ripudiabile
- Inalterabile e illegibile

32) Che cosa si intende per "CSI Effect"?

- Il modo in cui alcune serie televisive hanno cambiato la percezione verso la prova informatica
- Un particolare filtro
- La capacità di applicare metodi scientifici ad alto contenuto tecnologico

33) L'enhancement del contrasto attraverso una tecnica di equalizzazione:

- Modifica l'istogramma distribuendo in maniera più uniforme le varie tonalità di segnale
-

34) Quale fra le seguenti modalità di acquisizione più completa nel settore della Mobile Forensics

- Acquisizione fisica
- Acquisizione logica
- Altro
- Acquisizione rubrica e chat

35) Quale tecnica di riduzione del rumore è la più indicata nel caso di rumore periodico?

- Passa banda in frequenza
- Filtro mediano
- Filtro gaussiano 3x3
- Filtro gaussiano 9x9
- Filtro media
- Altro

36) Quale dei seguenti accertamenti è rivolto al ritrovamento del corpo del reato o cose pertinenti al reato?

- Ispezione informatica
- Perquisizione informatica
- Sequestro
- Copia bit a bit

37) Quale fra i seguenti elementi può essere omesso nella redazione di una consulenza tecnica informatica

- Quesito
- Conclusioni
- Allegati Tecnici
- Analisi
- Firma

38) Tecniche di zooming

- Aumentano la dimensione dell'immagine applicando apposite tecniche di interpolazione
- Migliorano il livello di dettaglio
- Migliorano la resa cromatica
- Migliorano la risoluzione effettiva

39) Standard, metodologie e best practice per la Digital Forensics. Quale delle seguenti normative/ standard specifica nel dettaglio le proedure da seguire?

- ISO9001
- ISO27001
- Codice per l'amministrazione digitale
- Legge 48 del 2008
- ISO 27037/27041/27042

40) Definizione di Slack Space:

- Area compresa tra l'ultimo bit allocato e la fine del settore non utilizzata dal file che ha allocato (Vera)