**Prova in Itinere – Digital Forensics – 5 Maggio 2022**

1. **Come può essere affrontato l'ipotetico problema delle collisioni della funzione di hash?**
   * 1. utilizzando 2 differenti funzioni hash contemporaneamente
     2. utilizzando la una funzione crittografica al posto dell’hash
     3. non è possibile far fronte a questo problema
     4. calcolando inizialmente l'hash del dato e successivamente un'ulteriore hash sulla stringa hash già prodotta
2. **La nomina del CTP nei procedimenti giudiziari avviene a cura**
   1. del legale o direttamente dalla parte, dal Pubblico Ministero
   2. dagli Ufficiali di Polizia Giudiziaria
   3. del cancelliere del Tribunale
   4. dal Giudice
3. **In una attività di live forensics in azienda, prima di procedere alle attività di acquisizione, quale tra queste attività va svolta per prima?**
   1. Fare una privilege escalation
   2. Collegare subito un write blocker USB
   3. Effettuare un debriefing con il cliente e chiedere il supporto di un Amministratore di Sistema
4. **il c.p.p. all’art. 359 si riferisce ad accertamenti tecnici ripetibili. Se si sta operando in regime di art. 359, è possibile**:
   * 1. non effettuare la cifratura del dato digitale
     2. effettuare operazioni senza la presenza della controparte
     3. utilizzare software open source
     4. non effettuare il calcolo dell’hash del dato digitale
5. **Quale tra i seguenti elementi se presenti può essere utilizzato per garantire l’autenticità e l’esistenza di un messaggio di posta elettronica?**
6. La ricevuta di ritorno
7. La presenza e il relativo valore del campo DKIM
8. La presenza e il relativo valore del campo Message\_ID
9. La presenza nell’header di un indirizzo IP valido e di un indirizzo mail del mittente valido
10. **L’alibi informatico è :**
    1. Non falsificabile
    2. Una dimostrazione della presenza dell’imputato in un altro luogo rispetto alla esecuzione di un crimine dimostrata in maniera “rigorosa”
    3. Un altro metodo che negli anni le difese usano per instillare il dubbio che l’accusato non abbia commesso il fatto
    4. Accettato solo quando proviene da log di Social Network (Facebook, Instagram, ecc.)
11. **Nell’acquisizione sistema di video sorveglianza su DVR è consigliabile**
    1. Esportare i dati nel formato proprietario
    2. Esportare i dati in formati standard AVI, MP4, ecc.
    3. Visualizzare e salvare in JPEG solo i fotogrammi di interesse
    4. Procedere al sequestro del DVR ed eseguire una copia forense del disco
    5. Esportare i dati in formato JPEG
12. **La chain of custody è un'attività che si concretizza nelle fasi di:**
    1. Identificazione
    2. in tutte le fasi
    3. analisi
    4. identificazione e preservazione
13. **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:**
    * 1. Il file non è integro ma è autentico
      2. Il file non è autentico e non è integro
      3. Il file è autentico ed integro
      4. Il file non autentico ma è integro

#Da controllare

1. **Che ruolo ricopre l’avvocato di parte civile nel processo penale**
   1. Difesa delle parti danneggiate dal reato
   2. Ausiliario dell'avvocato difensore
   3. Giudice per le indagini preliminare (GIP)
   4. Ausiliario del consulente tecnico di parte
   5. Organo giudicante.
   6. Giudice a latere
   7. Pubblica Accusa
   8. Tribunale del Riesame
2. **Cos'è un meccanismo write blocker?**
3. un dispositivo che, dati un dispositivo sorgente e uno di destinazione, impedisca la scrittura sul dispositivo destinazione
4. un dispositivo che, dati un dispositivo sorgente e uno di destinazione, impedisca la scrittura sul dispositivo sorgente
5. qualsiasi sistema software o hardware che, dati un dispositivo sorgente e uno di destinazione, impedisca la scrittura sul dispositivo destinazione
6. qualsiasi sistema software o hardware che, dati un dispositivo sorgente e uno di destinazione, impedisca la scrittura sul dispositivo sorgente
7. **Quali sono le fasi della digital forensics?**
   1. sequestro-catena di custodia - analisi – dibattimento
   2. identificazione-preservazione-acquisizione-analisi-documentazione
   3. acquisizione - documentazione - analisi – presentazione
   4. individuazione-acquisizione - analisi - documentazione – presentazione
8. **In una attività di live forensics su Windows 10 aggiornato, quale serie di tool dovrà avere il consulente?**
   1. Snort
   2. Password Cracking
   3. Write blocker
   4. Chiavetta USB con collezione collaudata di tool live
9. **Quali delle seguenti affermazioni descrive al meglio le evidenze digitali?**
10. Le evidenze digitali sono volatili ed inalterabili.
11. Le evidenze digitali sono volatili, duplicabili e alterabili.
12. Le evidenze digitali sono duplicabili.
13. Le evidenze digitali rappresentano sempre dei fatti probatori durante l’iter

1. **Il c.p.p. all’art. 360 si riferisce ad accertamenti tecnici non ripetibili, in quali fasi della digital forensics può presentarsi?**
2. acquisizione-analisi
3. in tutte le fasi
4. sequestro-catena di custodia - analisi - dibattimento
5. individuazione-acquisizione - analisi - documentazione - presentazione
6. **Se apro un file con il software “MSWord” e lo richiudo senza apportare modifiche il valore della relativa funzione hash:**
   1. Non cambia
   2. Cambia solo se si usa SHA1
   3. Cambia solo se si esegue il comando “SALVA”
   4. Cambia solo se si usa MD5
   5. Cambia
7. **Quali tra queste problematiche possono verificarsi durante un'analisi “live”?**
8. difficoltà nell'eseguire le operazioni
9. impossibilità di costruire la chain of custody
10. perdita dei dati post analisi
11. perdita del fattore di ripetibilità delle operazioni
12. **La disciplina Multimedia Forensics si occupa di elaborare dati multimediali al fine di procedere con:**
13. Analisi, miglioramento, recupero di informazioni semantiche da reperti multimediali
14. Acquisizione, analisi e codifica
15. Analisi e Miglioramento segnali audio
16. Identificazione della sorgente di acquisizione e verifica di integrità dei reperti multimediali
17. Recupero targhe e analisi antropometriche
18. **In cosa consiste l'acquisizione tramite duplicazione/clone?**
    * + 1. creare una copia 1:1 del dispositivo sorgente su un supporto equivalente
        2. effettuare copia dei singoli dati presenti nel dispositivo sorgente e gli hash degli di questi ultimi
        3. copiare il contenuto del dispositivo sorgente in un generico supporto di grandezza equivalente
        4. creare una copia immagine del dispositivo sorgente
19. **Perchè, nella digital forensics, sono importanti le modalità di acquisizione e trattamento delle evidenze?**
    1. Per garantire la ripetibilità delle analisi
    2. Tutte le risposte sono corrette
    3. Per garantire l’autenticità della fonte di prova
    4. Perché si abbiano abbastanza elementi da portare come fonte di prova ai fini legali
    5. Per garantire sia l’autenticità della fonte di prova sia la ripetibilità delle analisi
20. **Elencare in ordine (crescente) di completezza e di accuratezza delle informazioni raccolte, le seguenti modalità di acquisizione nell’ambito della Mobile Forensics:**
    1. Screenshot, Logica, Fisica
    2. Fisica, Logica, Screenshot
    3. Logica, Fisica, Screenshot,
21. **I software di wiping riescono a cancellare anche i dati presenti nello “Slack Space”**
    * 1. Si
      2. Dipende dalle configurazioni di sistema e dai relativi protocolli di sicurezza
      3. In parte
      4. No
22. **La Perquisizione anche Informatica (Art 247 cpp) è:**
    1. Un mezzo di ricerca della prova volto al rintraccio del corpo di reato o di cose pertinenti al reato che una volta rinvenute devono essere sottoposte a sequestro
    2. Un accertamento irripetibile volto ad acquisire fonti di prova
    3. Un mezzo di ricerca della prova volto ad accertare le tracce del reato
23. **L’Ispezione anche Informatica (Art 244 cpp) è:**
    1. Un mezzo di ricerca della prova volto al rintraccio del corpo di reato o di cose pertinenti al reato che una volta rinvenute devono essere sottoposte a sequestro
    2. Un mezzo di ricerca della prova volto ad accertare le tracce del reato
    3. Un accertamento irripetibile volto ad acquisire fonti di prova
24. **Legge di Ratifica “Convenzione di Budapest” si riferisce a:**
    1. L. n. 59/199 (riconoscimento regolamentazione della validità dei documenti formati e/o trasmessi con strumenti informatici)
    2. DPR n. 68/2005 e DM 2 novembre 2005
    3. Legge n.48 del 18 marzo2008
    4. Codice dell’Amministrazione Digitale (cd. CAD) di cui al D. Lgs. 82/2005 e successive modificazioni
25. **Presupposti reato di Diffamazione in Rete**
    1. Assenza dell’offeso, Offesa all’altrui reputazione, Comunicazione a più persone
    2. Comunicazione a mezzo social network con contenuti diffamatori
    3. Presenza di messaggi privati lesivi della reputazione su piattaforme di messagistica
26. **Quali tra i seguenti elementi presenti in una relazione di Consulenza Tecnica possono essere omessi:**
    1. Metodologia di lavoro e Analisi Tecnica
    2. Testo del quesito e estremi del procedimento
    3. Dati anagrafici dei soggetti indagati
    4. Conclusioni
    5. Dati di lavoro (acquisizione, provenienza)
27. **Elencare in ordine decrescente di sicurezza le seguenti funzioni HASH:**
    1. Md-5, SHA-256, SHA-512
    2. SHA-256, SHA-512, MD-5
    3. SHA-512, MD5, SHA-256
    4. SHA-512, SHA-256, MD-5
28. **Valore legale messaggio di Posta Elettronica**
    1. Documento Informatico
    2. Documento informatico sottoscritto con firma digitale
    3. Nessuna validità a seguito della impossibilità di garantirne l’integrità, la paternità e altre caratteristiche correlate.
    4. Documento informatico sottoscritto con firma semplice
29. **Caratteristiche PEC:**
    1. Integrità del Messaggio, Certificazione dell’Invio, Certificazione della Consegna
    2. Integrità degli Allegati, Certificazione del Mittente, Certificazione della Consegna
    3. Integrità degli Allegati, Certificazione dell’Invio, Certificazione del Destinatario
    4. Integrità del Messaggio, Certificazione del Mittente, Certificazione della Consegna

**DIGITAL FORENSICS Prova in ITINERE del 5 Maggio 2022**

Cognome\_\_\_\_\_\_\_\_\_\_\_\_ NOME\_\_\_\_\_\_\_\_\_\_\_ MATRICOLA: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

|  |  |
| --- | --- |
| **Quesito** | **Risposta** |
| **1** |  |
| **2** |  |
| **3** |  |
| **4** |  |
| **5** |  |
| **6** |  |
| **7** |  |
| **8** |  |
| **9** |  |
| **10** |  |
| **11** |  |
| **12** |  |
| **13** |  |
| **14** |  |
| **15** |  |
| **16** |  |
| **17** |  |
| **18** |  |
| **19** |  |
| **20** |  |
| **21** |  |
| **22** |  |
| **23** |  |
| **24** |  |
| **25** |  |
| **26** |  |
| **27** |  |
| **28** |  |
| **29** |  |
| **30** |  |