Digital Forensics – Luglio 2022

NOME: Gaia Natalj COGNOME: Contino
MATRICOLA: 1000042354

Email:gaianataljcontino97@gmail.com

- Reati Informatici
- Chain of Custody
- Legge 48 del 2008

1) **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

2) **I software di wiping riescono a cancellare anche i dati presenti nello "Slack Space"**
   a. No
   b. Si
   c. Dipende dalle configurazioni di sistema e dai relativi protocolli di sicurezza
   d. In parte

3) **La nomina del CTP nei procedimenti giudiziari avviene a cura**
   a. del legale o direttamente dalla parte, dal Pubblico Ministero
   b. dal Giudice
   c. del cancelliere del Tribunale
   d. dagli Ufficiali di Polizia Giudiziaria

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**:
   a. non effettuare il calcolo dell'hash del dato digitale
   b. effettuare operazioni senza la presenza della controparte
   c. non effettuare la cifratura del dato digitale
   d. utilizzare software open source

5) **Quale tra i seguenti elementi se presenti può essere utilizzato per garantire l'autenticità e l'esistenza di un messaggio di posta elettronica?**
   a. La presenza e il relativo valore del campo DKIM
   b. La presenza e il relativo valore del campo Message_ID
   c. La ricevuta di ritorno
   d. La presenza nell'header di un indirizzo IP valido e di un indirizzo mail del mittente valido

6) **L’alibi informatico è :**
   a. Non falsificabile
   b. Una dimostrazione della presenza dell’imputato in un altro luogo rispetto alla esecuzione di un crimine dimostrata in maniera “rigorosa”
   c. Accettato solo quando proviene da log di Social Network (Facebook, Instagram, ecc.)
   d. Un altro metodo che negli anni le difese usano per instillare il dubbio che l’accusato non abbia commesso il fatto

7) **Che ruolo ricopre l’avvocato di parte civile nel processo penale**
   a. Ausiliario dell'avvocato difensore
   b. Giudice per le indagini preliminare (GIP)
   c. Ausiliario del consulente tecnico di parte
   d. Tribunale del Riesame
   e. Organo giudicante.
   f. Giudice a latere
   g. Pubblica Accusa
   h. Difesa delle parti danneggiate dal reato

8) **Nell’acquisizione sistema di video sorveglianza su DVR è consigliabile**
   a. Esportare i dati nel formato proprietario
   b. Esportare i dati in formati standard AVI, MP4, ecc.
   c. Procedere al sequestro del DVR ed eseguire una copia forense del disco
   d. Esportare i dati in formato JPEG
   e. Visualizzare e salvare in JPEG solo i fotogrammi di interesse

9) **La chain of custody è un'attività che si concretizza nelle fasi di:**
   a. Identificazione
   b. Analisi
   c. in tutte le fasi
   d. identificazione e preservazione

10) **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:**
   a. Il file non autentico ma è integro
   b. Il file non è autentico e non è integro
   c. Il file è autentico ed integro
   d. Il file non è integro ma è autentico

11) **Cos'è un meccanismo write blocker?**
   a. un dispositivo che, dati un dispositivo sorgente e uno di destinazione, impedisca la scrittura sul dispositivo destinazione
   b. un dispositivo che, dati un dispositivo sorgente e uno di destinazione, impedisca la scrittura sul dispositivo sorgente
   c. qualsiasi sistema software o hardware 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 sorgente

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

13) **Quali sono le fasi della digital forensics?**
    a. sequestro-catena di custodia - analisi - dibattimento
    b. individuazione-acquisizione - analisi - documentazione - presentazione
    c. identificazione-preservazione-acquisizione-analisi-documentazione
    d. acquisizione - documentazione - analisi – presentazione

14) **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

15) **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 una LUT
    f. Applicare un filtro nel dominio della frequenza

DIGITAL FORENSICS Prova in ITINERE del 13 Luglio 2022

Cognome: Contino NOME: Gaia Natalj MATRICOLA: 1000042354

Quesito	Risposta
1	A
2	B
3	A
4	B
5	A
6	B
7	H
8	C
9	C
10	D
11	D
12	A
13	C
14	B
15	B

Reati informatici:

Con reati informatici si intende commessi per mezzo dell'elaboratore elettronico e dei programmi in esso installati quindi con l'utilizzo di tecnologie informatiche o telematiche, reati commessi a danno degli elaboratori, dei programmi e dei dati in essi contenuti. Esiste un terzo genere di crimini informatici in cui il soggetto agente è proprio il sistema informatico.

Chain of Custody:

La catena di custodia è il documento che deve permettere a posteriori di verificare le operazioni svolte e tiene traccia dei dettagli dei reperti informatici.

Per ogni reperto, sono indicati cronologicamente i diversi attori che hanno trattato il dato informatico e le operazioni svolte.

Le sue procedure sono:

-Tenere un registro che mostri quando le prove sono state ricevute e sequestrate e dove queste si trovano.

-Registrare le date se gli oggetti sono rilasciati a qualcuno.

-Limitare l'accesso alle prove.

-Collocare il disco rigido originale in un armadietto delle prove
-Eseguire tutte le analisi forensi su una copia dell'immagine speculare, mai sui dati originali.

Legge 48 del 2008:

La legge 48 del 2008 è la legge di Ratifica "Convenzione di Budapest".
è una legge sulla criminalità informatica e riguarda i crimini commessi attraverso internet o altre reti informatiche.