10 giugno 2023 – Qualification Test

Domande teoriche

1) Qual è la funzione principale dell'hashing in digital forensics?
a) Tutelare la privacy dei dati
b) Comprimere i dati
c) Garantire l'integrità dei dati

2) Quale strumento è usato comunemente per l'analisi forense della memoria in sistemi Windows?
a) FTK Imager
b) Volatility
c) Wireshark

3) Qual è il processo di raccolta di prove digitali da un sistema informatico acceso?
a) Dead-box forensics
b) Live forensics
c) Network forensics

4) Quale dei seguenti formati di immagine forense è utilizzato comunemente in digital forensics?
a) JPEG
b) EWF
c) BMP

10 giugno 2023 – Qualification Test

5) Quale tool può essere utilizzato per l'acquisizione di immagini forensi di un disco?
a) Autopsy
b) FTK Imager
c) log2timeline/plaso

6) Cosa indica l'acronimo MFT in un contesto NTFS?
a) Main File Transfer
b) Master File Table
c) Massive Format Type

7) A cosa serve l'Indice $I30 in NTFS?
a) Elenca i file eliminati ma ancora recuperabili
b) Elenca i file presenti nella directory che lo contiene
c) Elenca i file crittografati

8) Cosa indica l'acronimo MAC in un contesto di Timeline Analysis?
a) Media Access Control
b) Modified, Accessed, and Created times
c) Machine Automated Code

9) Quale tecnica può essere utilizzata per recuperare dati da un hard disk che è stato formattato?
a) Deep web scraping
b) Data carving
c) Quantum computing

10 giugno 2023 – Qualification Test

10) Cosa rappresenta un file di paging o swap per un informatico forense?
a) Un luogo dove sono memorizzati i file nascosti
b) Un luogo dove il sistema operativo salva dati della memoria RAM
c) Una memoria cifrata

11) Qual è il protocollo più comune utilizzato per acquisire prove digitali da dispositivi di rete?
a) TCP/IP
b) FTP
c) NetFlow

12) Quali informazioni possono essere recuperate dai metadati di una foto digitale?
a) Data e ora di scatto, modello della fotocamera, coordinate GPS
b) Nome del fotografo, dimensioni del file, tipo di compressione
c) Titolo della foto, descrizione, tag dei volti

13) Cosa si intende per "forensic imaging" durante l'acquisizione di prove digitali?
a) Creazione di una copia esatta bit per bit di un dispositivo o di una partizione
b) Analisi dei contenuti di un dispositivo senza crearne una copia
c) Creazione di una copia di backup dei file importanti

14) Qual è il principale obiettivo dell'analisi forense di rete?
a) Identificare vulnerabilità di sicurezza
b) Recuperare dati persi
c) Analizzare il traffico di rete

10 giugno 2023 – Qualification Test

15) Cosa si intende per "volatility analysis" nell'analisi forense digitale?
a) Analisi delle modifiche dei file nel tempo
b) Analisi delle tracce di attività di rete
c) Analisi delle informazioni contenute nella memoria di un sistema

16) Qual è lo scopo dell'utilizzo di un "write blocker" durante l'acquisizione di prove digitali?
a) Prevenire modifiche accidentali ai dati originali
b) Aumentare la velocità di acquisizione dei dati
c) Creare una copia crittografata dei dati acquisiti

17) Quale dei seguenti non è un metodo comune per l'acquisizione di prove digitali?
a) Imaging forense
b) Copia di backup
c) Copia di file casuali

18) Cos'è un hash MD5 utilizzato nell'analisi forense digitale?
a) Un algoritmo crittografico
b) Un formato di file immagine
c) Un tipo di dispositivo di archiviazione

19) Cosa significa "metadata" nel contesto delle prove digitali?
a) Dati che descrivono altri dati
b) File multimediali come foto e video
c) Messaggi di posta elettronica

10 giugno 2023 – Qualification Test

20) È possibile che due file di testo abbiano lo stesso valore di hash se il contenuto è identico, ma il nome dei due file è differente?

a) Solo in alcuni casi specifici, per esempio se si tratta di file in formato “bin”

b) Sì, il nome del file non è influente per la funzione di hash. Il nome del file può essere considerato come una mera etichetta

c) No, perché cambiando il nome del file varia anche il valore di hash risultante

21) Supporta la creazione di snapshot a livello di file system:

a) NTFS

b) BTRFS

c) EXT4

22) Tramite quale dei seguenti comandi è possibile copiare il Master Boot Record di un disco?

a) dd if=/dev/sda of=/tmp/mbrsda.bak bs=512 count=1

b) dd if=/dev/sda of=/tmp/mbrsda.bak bs=512 count=512

c) dd if=/dev/sda of=/tmp/mbrsda.bak bs=512 count=0 status=progress

23) Le chiavi che definiscono un volume New Technology File System sono contenute all’interno:

a) del file di registro SAM

b) della Master File Table (MFT)

c) del file di registro SOFTWARE

10 giugno 2023 – Qualification Test

24) In uno smartphone Android, potrebbe essere sostituita facendo restare immutato il codice IMEI:

a) La partizione “Recovery” (sostituita con una partizione custom)

b) La scheda madre

c) Nessuna delle risposte precedenti

25) Quale dei seguenti hash corrisponde a quello di una password Windows vuota?

a) “31d6cfe0d16ae931b73c59d7e0c089c0”

b) “066ddfd4ef0e9cd7c256fe77191ef43c”

c) “7ddeb1fef70a3c01edbed115bf5bb8ba”

26) Un disco “OS” oggetto di sequestro, crittografato con “Bitlocker”, potrà essere sbloccato da un altro PC (differente da quello che lo ospitava e, dunque, con un TPM diverso):

a) Esclusivamente con la password dell’utente o la chiave di ripristino;

b) Esclusivamente con la chiave di ripristino;

c) Esclusivamente con la password dell’utente

27) NON è un codice di riconoscimento univoco per una catena di custodia:

a) Product Number

b) IMEI

c) MAC Address

10 giugno 2023 – Qualification Test

28) Un sistema mobile che fa uso della misura di sicurezza FRP

a) Permette all'utente del dispositivo di poter decidere quali dati possono essere condivisi tra le varie applicazioni

b) Permette all'utente del dispositivo di rendere lo stesso invulnerabile agli attacchi di tipo MITM

c) Permette all'utente che ha perso il dispositivo di mantenere al sicuro i suoi dati personali

29) Contengono informazioni utili che riguardano le modifiche effettuate su file e cartelle in ambiente Windows

a) $J, $LogFile

b) SAM, SYSTEM

c) NETUSER.dat, SECURITY

Domande su prove pratiche

30) In quale data è stata pubblicata la pagina web che compare per prima come risultato della seguente ricerca https://www.google.com/search?q=nuova+caine+13.0+warp (folder 01)?

a) 18 maggio 2015

b) 12 marzo 2017

c) Tra il 7 e il 18 maggio 2023

31) La mail contenuta nel folder 02 è originale o è stata modificata?

a) è stata davvero inviata da hackinbo@virgilio.it ad hackinbo@protonmail.com con quel testo

b) è stata davvero inviata da hackinbo@virgilio.it con quel testo esatto ma non ad hackinbo@protonmail.com

c) non è possibile stabilirlo, non avendo accesso al server ma potendo contare soltanto su un file EML che non è poi altro che un semplice file di testo

10 giugno 2023 – Qualification Test

32) Con quale software e quando è stato creato il pdf "privacy.pdf "contenuto nel folder 03?
a) Il pdf non contiene metadati
b) Con LibreOffice 7.1 il 4 maggio 2021
c) Non è ricostruibile il software ma la data è febbraio 2020

33) E' stata riconsegnata, in un'azienda, una microSD formattata: al suo interno non ci sono più i documenti aziendali di prima, ma al loro posto soltanto due file di testo. Il reparto IT sta cercando di capire in quale data e ora locale questa sia stata formattata. Avendo a disposizione la copia forense puoi ipotizzare che tale ripristino sia avvenuto:
a) il giorno 8 giugno 2023 alle ore 15:13:59
b) il giorno 8 giugno 2023 alle ore 14:15:04
c) il giorno 8 giugno 2023 alle ore 13:13:59

34) Sono stati sequestrati 3 dispositivi nell'ambito di un procedimento penale. E' necessario identificare da quale dei 3 dispositivi è stata scattata una fotografia rinvenuta su una pendrive recapitata in procura anonimamente, che contiene nei metadati EXIF il dettaglio di un modello di smartphone che l'indagato non possiede: da quale dei seguenti dispositivi è stata scattata invece la fotografia?
a) iPhone 13
b) iPhone 8
c) iPhone 12