1) Dare una definizione di informatica forense.

L'informatica forense è la disciplina che concerne le attività di individuazione, conservazione, protezione, estrazione, documentazione ed ogni altra forma di trattamento ed interpretazione del dato memorizzato su supporto informatico, al fine di essere valutato come prova nel processo.

2) Illustrare la rilevanza dell'adozione best practice nell'ambito dell'informatica forense.

Solo supportando le attività di accertamento con un rigoroso percorso metodologico il consulente tecnico potrà confermare oggettivamente le proprie conclusioni attraverso la prova di resistenza. Inoltre, l'utilizzo di pratiche attendibili, riconosciute dalla comunità scientifica, permette una maggiore credibilità di fronte al giudizio rendendo più solide le proprie argomentazioni.

3) Quali sono i limiti e le criticità dell'informatica forense?

Data l'estrema alterazione dei reperti informatici, la facile creazione ad arte di elementi probatori e la difficile riconducibilità dei reperti ai veri autori è necessario capire che il trattamento dei dati dell'informatica forense è estremamente critico. Pertanto, è necessaria una profonda attività di autocritica in quanto il reperto informatico è spesso ingannevole e bisogna cercare in maniera paranoica elementi di riscontro.

4) Cosa individua un indirizzo IP nel contesto dell'informatica forense?

L'indirizzo IP nell'informatica forense individua univocamente in un preciso istante un sistema in una rete, o meglio un'utenza telefonica. Questo però non risulta un sufficiente elemento di prova senza aver prima accertato che non vi siano state manomissioni nelle architetture stesse della rete, ad esempio con abusivi collegamenti ad un'utenza di proprietà altrui.

5) Spiegare le differenze tra data di ultimo accesso e data di ultima modifica dei file e fare un esempio di come si possono utilizzare.

La data di ultimo accesso ad un file indica l'ultima volta che questo è stato aperto (anche copiato), l'ultima modifica invece specifica l'ultima volta che questo file è stato aggiornato (in particolari casi gli orari di accesso, modifica e creazione possono coincidere). Questi non danno una prova certa dell'orario di avvenimento poiché potrebbero essere modificati ad arte, ma per fare un esempio potrebbero essere utilizzati per creare una timeline di utilizzo del dispositivo per rilevare un evento di copia massiva di file. Bisogna sempre ricordare che è necessario cercare altri elementi di riscontro per combinare più indizi in una prova.

6) Indicare il comando che permette di eseguire il wiping di un reperto identificato come /dev/sda.

```
for i in {1..7}
do
    dd if=/dev/zero of=/dev/sda bs=16M
done
```

7) Quale deve essere il ruolo del consulente tecnico?

Il ruolo di un consulente tecnico di informatica forense è quello di aiutare il giudice nell'investigare governando le tecnologie forensi mostrando elementi di prova del caso, senza mai sostituirsi al giurista.

8) Dare una definizione di mobile forensics.

La mobile forensics è quella branca dell'informatica forense che si occupa di identificare, preservare e analizzare dati informatici che possono assumere valore probatorio quando il dato è contenuto in un dispositivo mobile. In realtà non vi sono molte differenze dall'informatica forense più in generale, infatti è necessario prendere gli stessi accorgimenti riconosciuti dalle comunità scientifiche, adattandosi alle possibilità che il particolare dispositivo dà a disposizione.

9) Si genera un'immagine forense con hash X; dopo due anni si verifica l'immagine forense e ritorna hash Y; indicare se è una condizione normale o in caso contrario quali possono essere le ragioni.

Avendo riscontrato che l'hash calcolato sulla stessa immagine forense risulta essere diverso due anni dopo la sua prima acquisizione ne risulta che il reperto non è in una condizione normale e la ragione è che probabilmente vi sono state delle manomissioni durante il periodo di conservazione del reperto. Bisognerebbe quindi valutare tutti i passaggi della catena di custodia e capire in quanto fosse sicuro il luogo in cui veniva conservata la prova, chi poteva averne accesso e chi tra questi avrebbe potuto ricavare dei vantaggi contraffacendola.

10) Descrivere cosa permettono di fare i seguenti comandi di linux: pwd, ls, dd, mkdir.

Quelli elencati sono alcuni dei comandi fondamentali utilizzabili con la shell di Linux. Il comando pwd (print working directory) ritorna in uscita sullo standard output la cartella in cui si sta lavorando in quel momento; ls (list directory) crea una lista con tutti i contenuti della directory attuale ed è possibile utilizzare alcune opzioni ad esempio per avere più informazioni; il comando dd ha come scopo principale quello di convertire e copiare file da una sorgente ad una destinazione o può essere utilizzato per effettuare wipe di dispositivi; mkdir (make directory) crea una nuova cartella con il nome indicato.

11) Definire cosa si intende per presunzione di repudio.

Data la natura dei documenti informatici bisogna valutare l'effimero valore probatorio del bit e pertanto, ogni dato informatico andrebbe presuntivamente considerato come modificato ad arte, dando alla parte interessata il dovere di dimostrarne l'attendibilità nel processo.

12) Spiegare quali sono e a cosa servono le fasi di trattamento del dato informatico.

Le fasi di trattamento del dato informatico sono: identificazione, raccolta (acquisizione conservazione traporto), analisi, valutazione, presentazione. L'identificazione è la prima fase che si pone di individuare tutti i dispositivi che possono contenere dati digitali. Nella fase di raccolta ci si pone di acquisire, conservare e trasportare in modo corretto le prove individuate, per fare questo vengono utilizzati appositi strumenti tecnici e viene documentato tutto anche mediante la catena di custodia. La fase di analisi viene effettuata su una copia dei dati originali e serve a ricostruire eventi passati utilizzando la regola delle 5W. Nelle ultime due fasi vengono interpretate mediante la scala di Casey le prove acquisite per giungere ad una conclusione presentandola in dibattimento per via scritta o orale rendendola comprensibile per chi non è del settore.

13) Descrivere le fasi di acquisizione live e post-mortem.

Nei casi di acquisizione è necessario prendere determinati accorgimenti necessari ad immortalare lo stato del dispositivo al momento del ritrovamento. La prima operazione da effettuare è fare una fotografia dello schermo, poi bisogna verificare informazioni (ora di sistema, cifratura, registri, processi in esecuzione, connessioni attive e porte aperte) ed acquisire la memoria RAM (dump). Una volta effettuate queste operazioni preliminari bisogna decidere se è meglio spegnere o staccare il dispositivo dall'alimentazione per poteri acquisire tutti i restanti dati successivamente. È importante specificare che con questa operazione vi è una piccola perdita di dati che purtroppo non risulta eliminabile, ma permette di superare situazioni critiche. Per quanto riguarda l'acquisizione post-mortem è necessario utilizzare alcuni strumenti tecnici (come write blocker, supporti wiped) per garantire l'attendibilità dei dati. È buona prassi documentare ogni singola operazione (anche l'ambiente di lavoro) tra queste se non viene utilizzato un copiatore hardware è necessaria una distribuzione software di informatica forense anche per calcolare il digest dell'acquisizione ed applicarne una marca temporale con sigillo elettronico. Infine, si passa alle operazioni di trasporto con la stesura della catena di custodia.

14) Spiegare a cosa serve la timeline e come la si può acquisire.

La timeline identifica gli eventi relativi ad i file conservati sul dispositivo che si sta analizzando, la sua versione più semplice viene effettuata affiancando in diagrammi i dati raccolti riguardo creazione, accesso e modifica dei file ad esso associati. Questo serve a identificare in ordine cronologico le operazioni effettuate sul dispositivo e permette ad esempio di riconosce facilmente copie massive di file. Non bisogna mai dimenticare che le date possono essere contraffatte, quindi è necessario acquisire più riscontri riguardo agli indizi raccolti.

15) Elencare quali strumenti si possono utilizzare per l'analisi nell'informatica forense.

Gli strumenti utilizzabili per l'analisi nell'informatica forense sono Autopsy, EnCase, FTK, Internet Evidence Analyzer, Oxygen Forensics, P2C. Inoltre, è possibile utilizzare timeline e supertimeline sul dispositivo oppure effettuare una serie di operazioni chiamate "link analysis" che permettono di collegare eventi acquisiti da fonti differenti in un unico quadro sinottico delle vicende accadute.

16) Cos'è la scala di certezza di Casey?

La scala di certezza di Casey si propone di fornire un criterio di valutazione delle prove digitali, è importante affidarsi alle considerazioni di questa scala dal momento che è difficile valutare l'attendibilità delle prove. Da tale scala vengono definiti 7 livelli di certezza che indicano quanto una prova possa essere affidabile a partire dal C0 (errato) fino ad arrivare al C6 (certo), fra di essi gli altri livelli sono: molto incerto, un po' incerto, possibile, probabile e quasi certo.

17) Cosa sono le fasi destruens e costruens di una consulenza tecnica?

Le relazioni tecniche vanno articolate in due fasi, la prima viene tipicamente chiamata destruens ed è atta a demolire e criticare le analisi tecniche svolte dal consulente tecnico di controparte. La seconda fase è quella chiamata costruens dove basandosi sugli accertamenti oggettivi svolti dalla controparte si arriva ad esprimere conclusioni diverse e favorevoli alla propria parte.

18) Quali sono gli strumenti di cattura di immagine forense e come si può rendere riproducibile un accertamento tecnico?

Per acquisire dati conformi all'informatica forense ovviamente non è possibile effettuare un semplice "copia e incolla" per questo proposito vi sono due possibilità che consistono nel creare un'immagine forense oppure un clone. È quindi necessario utilizzare appositi copiatori hardware oppure il comando dd su un'apposita distribuzione forense di linux per effettuare un clone del disco da acquisire, invece, per creare un'immagine forense è possibile utilizzare dei software, ad esempio FTK Imager su sistemi Windows e Guymager su sistemi linux.

19) Cosa si intende per data carving?

Per data carving si intendono quelle tecniche utilizzate per recuperare dati eliminati allocati nel file system e non sovrascritti all'interno dello slack space. Si può effettuare il data carving utilizzando appositi strumenti che vanno a cercare porzioni di file del disco con i loro indici associati nella tabella del file system.

20) Quali sono i passi di acquisizione forense di un sito web?

La corretta acquisizione forense di un sito web è più complessa di quanto si potrebbe pensare normalmente. Per poterla effettuare bisogna eseguire diversi passi: 1) utilizzare una macchina virtuale con una distribuzione linux di tipo forense; 2) avviare una procedura di registrazione audio e video delle operazioni eseguite; 3) avviare una procedura di intercettazione del traffico di rete generato dalla macchina virtuale; 4) consultare un sito dal quale poter documentare la data di inizio dell'acquisizione; 5) consultare tutte le pagine da acquisire in modo manuale oppure utilizzare strumenti per acquisirne porzioni in maniera automatica; 6) consultare nuovamente un sito dal quale poter documentare la data di fine dell'acquisizione; 7) chiudere la procedura di intercettazione del traffico di rete e della registrazione audio-video; 8) spegnere la macchina virtuale; 9) generare un archivio compresso contenente i file della macchina virtuale, la registrazione audiovisiva, il file di traffico di rete ed i singoli file delle pagine web; 10) calcolare l'hash dell'archivio compresso; 11) applicare una marca temporale all'hash calcolato.

21) Dare una definizione di network forensics.

La network forensics è quella branca dell'informatica forense che si occupa di identificare, preservare e analizzare dati informatici che possono assumere valore probatorio quando il dato è in transito in una rete informatica.

22) Definire il cloud computing con i suoi diversi modelli e cosa comporta per l'informatica forense.

Il cloud computing è quella tecnologia che consente di usufruire, tramite server remoto, di risorse software e hardware il cui utilizzo è offerto come servizio da un provider. Vi sono diversi modelli, quali SaaS, PaaS e IaaS che si contraddistinguono dallo specifico servizio offerto, rispettivamente una piattaforma software pronta, risorse hardware da usare per lo sviluppo di applicazione e infine, data center virtuali a disposizione dell'utente. Inoltre, possiamo distinguere i tipi di cloud fra pubblico, privato oppure ibrido. Per quanto riguarda l'informatica forense il contro è principalmente la difficoltà di accesso ai dati di interesse, mentre come pro vi è l'alta probabilità che i dati verranno conservati e ne potremo anche trovare diverse copie.

23) Descrivere problemi, vantaggi e modalità di intercettazioni telematiche.

Le intercettazioni telematiche vengono sempre effettuate a basso livello, quindi all'accesso della rete, queste possono essere a bersaglio o parametriche ponendo una sonda vicino al bersaglio da intercettare. Vi sono due principali problemi in questo ambito: i collegamenti cifrati che le rendono inefficaci e le difficili definizioni di pattern per riuscire a prendere tutti i dati corretti. Per quanto riguarda le modalità è possibile effettuare una ricerca "live" in tempo reale che richiede però molta potenza computazionale, oppure effettuare memorizzazione e ricerca che suppone l'avere disponibile molta memoria di archiviazione. Il vantaggio scaturito dalle intercettazioni è la possibilità di ottenere informazioni senza dover accedere fisicamente al luogo del sistema monitorato.

24) Descrivere l'attendibilità dei reperti su dispositivi mobili.

I dispositivi mobili nell'informatica forense vanno considerati come qualsiasi altro dispositivo per quanto riguarda la validità dei reperti trovati al suo interno, sotto certi aspetti essendo sistemi molto diversi comportano persino maggiori criticità (ad esempio nell'acquisire dati evitandone la modifica). Vi sono infatti diversi strumenti, applicazioni o siti web che permettono di falsificare i dati relativi ai contenuti come chiamate o messaggi e per questo motivo è necessario effettuare controlli incrociati su diversi dispositivi per considerare un reperto attendibile a tutti gli effetti.

25) A cosa servono le linee di handover per l'informatica forense?

Le linee di handover nell'informatica forense potrebbero essere utilizzate per acquisire dati riguardo la geolocalizzazione di un utente in un dato momento e forniscono però dati pressoché approssimativi che andrebbero verificati con molteplici riscontri. Per linee di handover si intendono quegli spazi oltre il quale avviene il passaggio da una cella ad un'altra, a seconda della disposizione delle stazioni radio base (BSS) vengono infatti suddivise in celle le coperture sul territorio.

26) Dare una definizione di embedded forensics.

La embedded forensics è quella branca dell'informatica forense che si occupa di identificare, preservare e analizzare dati informatici che possono assumere valore probatorio quando il dato è contenuto in particolari dispositivi orientati ai servizi.

27) Come si può dimostrare l'inattendibilità di un documento stampato come elemento di prova?

Per dimostrarne l'inattendibilità di un documento stampato basterebbe ricreare ad arte un documento uguale. Dato l'effimero valore probatorio del bit, bisogna considerare la modifica di un dato informatico sempre come avvenuta. A maggior ragione, un documento stampato non può avere alcun valore probatorio se la parte interessata non ne dimostra l'autenticità.

28) Descrivere gli elementi di una catena di custodia e la sua utilità nell'informatica forense.

Serve a comprendere se i processi di acquisizione sono corretti, documentare accuratamente le operazioni eseguite per l'acquisizione di dati volatili e non volatili. Può essere effettuata con un documento per ogni reperto informatico o per tutti i reperti informatici di uno stesso caso. È importante per identificare i soggetti che hanno in custodia i reperti digitali, consente la conoscenza della continuità della custodia, prova l'integrità della gestione dei reperti raccolti. Indica data ed ora del sequestro, luogo e persone da cui si è prelevato, dati del dispositivo prelevato, nome delle persone che hanno raccolto il sequestro, nome e firma di tutte le persone che ricevono i reperti, numerazione e classificazione interna del reperto, dati tecnici pertinenti e valori del digest.

29) Si può considerare attendibile come elemento di prova una email stampata? Giustificare la risposta.

La stampa di una mail ricevuta di per se non può essere considerata come un elemento di prova attendibile, questo per diversi motivi: c'è la possibilità che sia stata creata ad arte; dalla stampa non è possibile avere riscontri riguardanti i metadati contenuti dalla stessa; inoltre è necessario verificare l'autenticità della mail controllando in modo approfondito tutti i dispositivi mittente e destinatari per cercare riscontri che permettano di utilizzare tali dati come prove in un processo; infine bisogna sempre pensare che chi ha inviato la mail potrebbe poi non essere stato chi viene accusato, ma qualcuno che ne poteva avere interesse.

30) Descrivere le differenze di acquisizione tra immagine forense fisica e logica, con i relativi vantaggi e svantaggi.

Un'immagine forense fisica consiste nell'estrazione di una copia di tutti i dati in un dispositivo di memorizzazione effettuata bit a bit in un formato clone o "imagine" verificabile mediante algoritmi di hash. Questa soluzione è sempre idonea, ma relativamente lenta, perciò in casi di necessità (es. copia di enormi quantitativi di dati in poco tempo) potrebbe non essere la soluzione migliore. L'immagine forense logica consiste nella copia dei file rilevanti salvati in un dispositivo di memorizzazione in un formato "imagine", in questo caso vi è una velocità maggiore nell'acquisizione dell'immagine forense a discapito però vi è perdita di informazione (dati cancellati, frammenti di file, informazioni riservate).

31) Quando può essere considerato attendibile un dato informatico?

Un dato informatico può essere considerato pienamente attendibile solo se vengono effettuati tutti gli opportuni controlli utilizzando le best practice che permettono di valutarne autenticità ed integrità. Alcuni strumenti necessari (ma non sufficienti) a considerare un documento informatico attendibile sono firma digitale, marca temporale e posta elettronica certificata.