SAMUELE PADULA 22/07/2023 ESAME DI DIGITAL FORENSICS

1. Proceda il Consulente Tecnico all'analisi forense del sistema informatico della società Hit & Run srl, al fine di stabilire se vi siano state intrusioni riconducibili alla società Catch All snc. In caso affermativo, verificare se siano stati sottratti alla Hit & Run srl documenti tecnici e/o altro materiale inerenti al brevetto delle "sneakers a rotelle a propulsione elettrica". Indicare le attività effettuate ai fini dell'indagine forense, nonché le ipotesi fatte, i dispositivi presi in considerazione, le applicazioni e/o i sistemi esaminati, le modalità di analisi effettuate (live / post-mortem / entrambe), ecc. e i risultati ottenuti da presentare al PM.

Seguendo quelli che sono i diversi step dell'analisi forense partiamo dalla

1. **Identificazione**: possiamo provare ad identificare le diverse fonti tra cui le segnalazioni di reato, eventuali ispezioni fisiche nei luoghi e uffici incriminati e interviste con possibili testimoni o soggetti interessati di ambo le parti. Si potrebbe partire con il localizzare le prove del crimine informatico elencando quelli che sono stati i sistemi utilizzati per commettere il crimine, come computer, telefoni cellulari, microspie e microfoni e i sistemi che sono stati danneggiati, sottratti o distrutti dal crimine (in questo caso Catch All snc) come server aziendali contenenti documenti tecnici o altro materiale inerente in questo specifico caso al brevetto delle "sneakers a rotelle a propulsione elettrica". Al fine di evidenziare un possibile rapporto tra l'azienda Hit & Run srl e la Catch All snc potremmo iniziare con il definire le relazioni tra le persone e i dipendenti, i sistemi ICT in uso nonchè le possibili connessioni esterne con eventuali aziende fornitori o partner di entrambe. In particolare in questa fase andiamo ad identificare tutte le fonti di prova potenziali, tra cui computer, telefoni cellulari (eventuali messaggi contenenti informazioni sul rilascio del nuovo brevetto/prodotto con date e luoghi annessi), dischi rigidi (contenenti i documenti potenzialmente sottratti), telecamere di sicurezza (per monitorare un eventuale accesso fisico alla struttura della Hit & Run srl da parte di personale non autorizzato) e altri dispositivi digitali. Una volta individuati i supporti digitali viene fatta un'analisi dei diversi elementi che concorrono al funzionamento di questi come la tipologia di SO, di file system, i tipi di file memorizzati. In questo caso un'analisi approfondita del sistema evidenzierebbe la presenza di diversi documenti realizzati dal team dell'ingegneria in formato di file multimediali e documenti office non cifrati salvati su un file server aziendale costituito da diverse interfacce di rete per il raggiungimento dalla sola LAN interna e diverse interfacce USB e firewire.
2. **Acquisizione e Conservazione:**

Il file server viene rinvenuto accesso dunque al fine di analizzare eventuali attività di esfiltrazione dei dati (analisi dei log di sistema, di rete, di accesso) non autorizzata si procede ad una analisi in modalità Live Forensics. Si potrebbe anche valutare in questo specifico caso di effettuare un'operazione di intercettazione (che in generale è più complessa in quanto richiede la tutela della riservatezza dei dati personali) per poter evidenziare se l'esfiltrazione è ancora in corso oppure è stato un evento singolo e sporadico. In questo caso si decide di effettuare prima un'analisi live e di analizzare eventuali log del sistema in quanto dalla visione delle telecamere di sicurezza sembrerebbe esserci stata l'intrusione di personale non autorizzato in un orario sospetto (in fase di chiusura degli uffici della Hit & Run srl) quindi è altamente probabile che i dati siano stati prelevati direttamente dal file server usando una delle interfacce presenti sul sistema. Inoltre in questo caso non potendo spegnere il sistema perché di primaria importanza per l'azienda l'analisi live risulta essere la scelta migliore. Procediamo dunque ad effettuare una copia dei log di sistema di eventuali porte USB o dispositivi che sono stati collegati al file server così da preservare il file di log originale che, essendo il file server in funzione, continua ad essere scritto dai diversi applicativi in funzione.

3. **Analisi e valutazione della fonte di prova:**

effettivamente da un analisi approfondita dei log risulta esserci stata l'introduzione di una chiavetta USB e un successivo IO rate elevato dovuto alla copia dei documenti sensibili. Dai log è risultato inoltre che alcuni metadati associati alla chiavetta USB avevano dei riferimenti alla società Catch All srl. Dopo ulteriori indagini presso gli uffici della Catch All srl e alcuni interrogatori si è comprovato l'accesso di un ex-dipendente della società Hit & Run srl (rilevato dalle telecamere di sicurezza) ed è stata rinvenuta la pennetta USB incriminata.

4. **Presentazione e Valutazione**: nel report di conclusione il consulente tecnico dettaglia le analisi che ha effettuato e le evidenze del caso in seguito anche all'attività della polizia giudiziaria tra cui la catena di custodia (in questo caso trattandosi di una chiavetta USB) e i risultati ottenuti. Se sono state trovate intrusioni o comunque prove riconducibili alla società Catch All snc allora il consulente deve fornire le prove della tesi sostenuta.

2. Fornire una definizione puntuale di "Computer Forensics" e descrivere le principali attività di tale disciplina, analizzando le varie fasi che costituiscono il ciclo di vita dell'evidenza digitale dal momento della sua identificazione fino alla chiusura del caso.

La computer forensics è una branca della scienza forense che si occupa dell'acquisizione, dell'analisi e della preservazione delle prove digitali. Dunque è un processo investigativo che fa uso di tecniche informatiche per identificare, acquisire, conservare e analizzare indizi o fonti di prova digitali. Le prove digitali possono essere utilizzate in una varietà di casi, tra cui reati informatici, frodi finanziarie, crimini violenti e incidenti industriali. Le prove digitali possono essere utilizzate per identificare il colpevole, ricostruire la scena del crimine e dimostrare la colpevolezza dell'imputato. Le prove digitali possono essere trovate in una varietà di luoghi, tra cui computer, telefoni cellulari, dischi rigidi, telecamere di sicurezza e altri dispositivi digitali. Gli investigatori possono utilizzare una varietà di tecniche per acquisire e analizzare le prove digitali, tra cui software forense, analisi manuale dei file e intervista con esperti. Le prove digitali possono essere un'importante fonte di informazioni per le indagini criminali. Possono aiutare gli investigatori a identificare il colpevole, ricostruire la scena del crimine e dimostrare la colpevolezza dell'imputato. Non esiste una definizione "formalizzata" di digital evidence, può essere definita come qualsiasi informazione avente valore probatorio che sia memorizzata o trasmessa in forma digitale.

La Computer Forensics prevede le seguenti fasi:

1. **Identificazione: Analisi preliminare, Ricerca delle fonti e Riconoscimento**
   Analisi preliminare
   la prima fase è l'identificazione delle prove digitali. Le prove digitali possono essere identificate da una varietà di fonti, tra cui segnalazioni di reato, ispezioni fisiche e interviste con testimoni.
   La prima fase dell'indagine è la valutazione del caso, che consiste nell'identificare il crimine e dove potrebbe essere localizzata la prova. Una volta identificata la prova, gli investigatori possono iniziare a indagare su due tipi di sistemi:

   - I sistemi utilizzati per commettere il crimine, come computer, telefoni cellulari e telecamere di sicurezza.
   - I sistemi che sono stati danneggiati o distrutti dal crimine, come computer, telefoni cellulari e telecamere di sicurezza.

   Gli investigatori possono utilizzare una varietà di tecniche per acquisire e analizzare le prove, tra cui software forense, analisi manuale dei file e intervista con esperti. Le prove possono essere utilizzate

per identificare il colpevole, ricostruire la scena del crimine e dimostrare la colpevolezza dell'imputato.
L'analisi preliminare a sua volta è costituita da 4 fasi principali:
1. Definizione della struttura organizzativa dell'indagato (le relazioni tra le persone, i sistemi ICT in uso, le possibili connessioni esterne e il numero di persone coinvolte)
2. Pianificazione e allocazione delle risorse (determinare il numero di personale da assegnare ai vari compiti, individuare e ingaggiare gli esperti forensi digitali nonché assegnare attrezzature e strumenti adeguati)
3. Stesura del contratto di ingaggio (Stabilisce un compenso sulla base del servizio offerto e permette di definire l'obiettivo della richiesta, le tempistiche e la remunerazione, la revisione della relazione prima della stesura del report finale o eventuali costi aggiuntivi relativi a ulteriori richieste)
4. Preparazione di una lista di testimoni/sospetti (La lista deve essere in parte fornita dal cliente e in parte individuata dall'esperto forense stesso)

Ricerca delle fonti e Riconoscimento

La ricerca delle fonti di prova e il riconoscimento sono le fasi iniziali di un'indagine forense digitale. In questa fase, l'investigatore deve identificare tutte le fonti di prova potenziali, tra cui computer, telefoni cellulari, dischi rigidi, telecamere di sicurezza e altri dispositivi digitali.

L'investigatore deve anche valutare l'utilità delle prove potenziali. Alcune prove possono non essere utili per l'indagine, mentre altre possono essere molto importanti. L'investigatore deve anche valutare il rischio di compromissione delle prove. Alcune prove possono essere facilmente compromesse, mentre altre sono più difficili da compromettere.

La ricerca delle fonti di prova e il riconoscimento sono fasi tecniche e importanti di un'indagine forense digitale. Queste fasi sono fondamentali per garantire che l'investigatore identifichi tutte le prove potenziali e le protegga dalla compromissione (cristallizzazione). Sta nell'esperienza e meticolosità dell'investigatore far emergere le casistiche. Ad esempio usando un approccio sistematico per identificare tutte le fonti di prova potenziali, valutandone l'utilità.
Inoltre alcune prove sono più facili da compromettere di altre dunque è necessario adottare le misure necessarie per ridurre il rischio di compromissione delle prove.

Una volta individuati i supporti digitali, è necessario capire dove cercare le prove. Per farlo, è necessario prendere in considerazione i diversi elementi che concorrono al funzionamento del sistema informatico, tra cui:

Tipologia del sistema informatico: questo fattore determina il principale utilizzo del dispositivo, che a sua volta influenza l'approccio da tenere nella ricerca. Ad esempio, un sistema informatico destinato agli utenti per attività ludiche o lavorative può essere spento, estratto dal disco e acquisito per intero. Un sistema informatico destinato all'erogazione di servizi critici o a supporto del business o dell'infrastruttura informatica, invece, non può essere spento e la duplicazione dei dati potrebbe essere gravosa. In questo caso, è necessario acquisire solo i dati che potrebbero essere fonte di prova, a sistema acceso.

Tipologia del sistema operativo: il sistema operativo è il cuore del sistema informatico e determina il tipo e il formato di file gestiti. Nel corso del suo funzionamento, il sistema operativo registra diverse informazioni in appositi file, salvati in posizioni note del file system. Queste informazioni possono

essere utilizzate per identificare le zone di memoria dove cercare i dati, tracciare l'uso del computer da parte dei diversi utenti ivi definiti, le periferiche che sono state collegate, l'elenco dei file stampati e su quale stampante, le reti (tradizionali o Wi-Fi) cui il computer è stato collegato e altro ancora.

Tipologia del file system: il file system determina come sono organizzati i dati archiviati e come li ospita. Esistono diversi tipi di file system, ognuno con le proprie caratteristiche. Alcuni dei file system più comuni sono ISO 9660, Joliet, CDFS, UDF, FAT 16/32, NTFS, EXT e QNX.

Tipologia di file: quando è noto cosa cercare, è possibile concentrarsi sui vari tipi di file. Esistono diverse tipologie di file che possono essere utili ai fini forensi, tra cui documenti, file di configurazione, file di log, file a supporto del sistema operativo, eseguibili e librerie, e file cifrati.

Presenza e tipologia di interfacce: il sistema informatico può essere dotato di diverse interfacce, come porte USB, porte FireWire, porte Ethernet, porte Wi-Fi e porte Bluetooth. Queste interfacce possono essere utilizzate per collegare il sistema informatico ad altri dispositivi, come computer, stampanti, scanner, dischi rigidi esterni e altri. È importante tenere conto della presenza e della tipologia di interfacce quando si cerca prove digitali, perché queste interfacce possono essere utilizzate per trasferire dati tra il sistema informatico e altri dispositivi.

2. **Acquisizione e Conservazione: Acquisizione ed Estrazione del dato e Conservazione**
   L'acquisizione di prove digitali è un processo complesso e delicato che richiede competenze tecniche e conoscenze specifiche. L'obiettivo è acquisire le prove digitali in modo valido e affidabile, in modo che possano essere utilizzate in un tribunale di giustizia.

   L'acquisizione delle prove digitali può essere eseguita in diversi modi, a seconda del tipo di dispositivo e delle prove che si stanno cercando. Alcuni metodi comuni di acquisizione di prove digitali includono:

   - Intercettazione: l'intercettazione è il processo di monitoraggio delle comunicazioni tra due o più dispositivi. L'intercettazione può essere eseguita su reti telefoniche, reti wireless e reti di computer.
   - Sequestro/Duplicazione: il sequestro è il processo di confisca di un dispositivo digitale. Il sequestro può essere eseguito con o senza il consenso del proprietario del dispositivo.
   - Acquisizione parziale del dato, se il sistema contiene troppi dati, solo alcuni casi sono rilevanti, solo alcuni dati possono essere acquisiti per vincoli legali

   L’approccio dipende anche dallo stato in cui viene ritrovato il sistema:
   Sistema spento (Post Mortem Forensics): l'analisi forense post mortem viene eseguita su un dispositivo digitale che è stato spento. Questo tipo di analisi è spesso utilizzato quando il dispositivo è stato danneggiato o quando è necessario preservare le prove. L'analisi post mortem può essere eseguita utilizzando una varietà di tecniche, tra cui la creazione di una copia bit-a-bit del dispositivo, l'analisi della memoria volatile e l'analisi dei file di registro.

   Sistema acceso (Live Forensics): l'analisi forense live viene eseguita su un dispositivo digitale che è acceso. Questo tipo di analisi è spesso utilizzato quando è necessario raccogliere dati in tempo reale o quando è necessario accedere a parti del dispositivo che non sono accessibili quando il dispositivo è spento. L'analisi live può essere eseguita utilizzando una varietà di tecniche, tra cui la scansione del dispositivo alla ricerca di malware, l'analisi del traffico di rete e l'analisi dei processi in esecuzione.

Inoltre quando si acquisiscono dati da un dispositivo digitale, è importante seguire alcune buone norme per garantire l'integrità delle prove. Queste buone norme includono:

Pulire il supporto utilizzato per la copia. Questo può essere fatto utilizzando un software di pulizia dati o formattando il supporto.

Validare la copia e verificarne l'integrità. Questo può essere fatto utilizzando una funzione di hash.

Tenere traccia degli aspetti temporali. Questo include la data e l'ora in cui è stata effettuata l'operazione, la sequenza con cui si sono verificate le azioni e lo scostamento temporale con gli orologi informatici.

Verifica dell'integrità della copia. Per verificare l'integrità di una copia, si può utilizzare la funzione di hash per calcolare il codice hash per il file originale e per il file copiato. Se i due codici hash sono uguali, allora i file sono identici. Se i due codici hash sono diversi, allora i file sono stati modificati.

Conservazione

Una volta acquisite le prove digitali, è necessario conservarle in modo sicuro. Le prove devono essere conservate in un luogo sicuro e protetto da alterazioni. Le prove devono essere conservate anche in un formato che possa essere facilmente accessibile agli investigatori.

La conservazione e la protezione della prova è una fase importante delle indagini forensi digitali. In questa fase, la prova deve essere protetta da alterazioni, deterioramento e accesso non autorizzato.

Ci sono una serie di misure che possono essere prese per proteggere la prova, tra cui:

- Sicurezza nel trasporto: la prova deve essere trasportata in modo sicuro e protetto, evitando l'esposizione a campi elettromagnetici, temperature estreme e umidità.

Protezione fisica dalle alterazioni: la prova deve essere protetta da danni fisici, come urti, cadute e acqua.

- Archiviazione sicura e replica: la prova deve essere archiviata in un luogo sicuro e protetto, lontano da fonti di calore, umidità e radiazioni.
- Restrizioni all'accesso al dato: l'accesso alla prova deve essere limitato a personale autorizzato.
- Catena di custodia: la catena di custodia è un documento che registra tutte le persone che hanno avuto accesso alla prova, le date e gli orari di accesso e le azioni eseguite sulla prova. La catena di custodia è importante per garantire l'integrità della prova e per dimostrare che la prova non è stata alterata.

3. **Analisi e valutazione della fonte di prova: Correlazione dei dati coi fatti**

Segue la fase di acquisizione (Live/ Post mortem) e conservazione dei dati e anche questa fase dipende dal contesto in cui si opera (es.operazioni di accertamento per la polizia/autorità giudiziaria, operazioni di accertamento in ambito aziendale) e consente di accertare eventuali attività di sabotaggio, di diffusione del codice malevolo o di violazione delle politiche aziendali. Questa fase comprende l’identificazione del supporto contenente le informazioni, il recupero dei file e delle informazioni cancellate, l’analisi del contenuto dei file e dei principali software applicativi

usando tool proprietari oppure open-source (CaineOS è un esempio di OS open-source per la digital forensics di cui abbiamo visto una simulazione di recupero dati steganografici durante le lezioni).

4. **Presentazione e Valutazione: Reportistica e Presentazione**
   I risultati e le conclusioni dell'indagine forense devono essere presentati in modo chiaro e conciso, in modo che possano essere facilmente compresi dal giudice e dalla giuria. L'esposizione deve anche essere solida dal punto di vista tecnico e deve resistere alle obiezioni dell'avversario.
   In tribunale, l'esperto forense sarà interrogato sia dalla parte che ha commissionato l'indagine (interrogatorio diretto) che dall'opposizione (contraddittorio). L'interrogatorio diretto è condotto dalla parte che ha commissionato l'indagine e ha lo scopo di fornire prove per dimostrare il caso. Il controinterrogatorio è condotto dall'opposizione e ha lo scopo di valutare la validità della testimonianza dell'esperto. Gli obiettivi dell'opposizione durante il controinterrogatorio sono:
   - Sminuire l'importanza della testimonianza diretta dell'esperto.
   - Ottenere dall'esperto delle testimonianze che sono favorevoli alla loro causa.

3. La figura dell'informatico forense è divenuta di grande importanza in ambito processuale quale consulente del giudice e delle parti nel settore delle evidenze digitali. Ciò premesso, indicare la diversa funzione dei mezzi di prova e dei mezzi di ricerca della prova spiegando la finalità e l'oggetto della perizia, la nomina da parte del giudice, facendo cenno all'attività del perito e a quella dei consulenti tecnici di parte.

I mezzi di prova sono gli elementi che consentono di accertare direttamente i fatti oggetto del processo. Sono previsti e disciplinati dal codice di procedura penale, ma è possibile utilizzare anche mezzi di prova atipici, se risultano idonei ad assicurare l'accertamento dei fatti e non pregiudicano la libertà morale della persona.

I mezzi di prova tipici qui elencati sono previsti e disciplinati dal codice di procedura penale:

- La testimonianza: è la dichiarazione resa da una persona che ha assistito al fatto oggetto del processo.
- L'esame delle parti: è l'interrogatorio delle parti in causa, che devono rispondere alle domande del giudice e delle altre parti.
- I confronti: sono le confrontazioni tra persone che hanno assistito al fatto oggetto del processo, per verificare se le loro dichiarazioni sono concordanti.
- Gli esperimenti giudiziali: sono le prove che vengono effettuate in tribunale, per ricostruire i fatti oggetto del processo.
- La perizia: è l'esame di un perito, che deve fornire al giudice una valutazione tecnica su un fatto oggetto del processo.
- I documenti: sono i testi, le immagini e gli altri supporti materiali che possono essere utilizzati come prove.

I mezzi di ricerca della prova sono invece:

- Le ispezioni: sono la ricerca di tracce, notizie o dichiarazioni rilevanti ai fini del processo.
- Le perquisizioni: sono la ricerca di beni o di persone rilevanti ai fini del processo, che possono essere eseguite solo con un ordine del giudice.
- I sequestri: sono il temporaneo o definitivo ritiro di beni o di persone rilevanti ai fini del processo.
- Le intercettazioni: sono l'ascolto e la registrazione di comunicazioni telefoniche o telematiche, che possono essere autorizzate dal giudice solo in casi particolari.

La perizia è un mezzo di prova che viene utilizzato per integrare le conoscenze del giudice con quelle di un esperto. L'esperto è una persona che ha una competenza specifica in un determinato campo, come la medicina, la chimica, la fisica, l'informatica o l'ingegneria.

Le finalità e oggetto della perizia sono normate dall'Art 220 del codice di procedura penale ed è ammessa quando occorre svolgere indagini o acquisire dati o valutazioni che richiedono competenze tecniche/scientifiche. Ad esempio, se in un processo si deve stabilire se un reato è stato commesso con un'arma da fuoco, il giudice può richiedere una perizia balistica.

Nel procedimento penale, il consulente tecnico del giudice è chiamato perito. Nel procedimento civile, il consulente tecnico del giudice è chiamato consulente tecnico d'ufficio (CTU). Sia nel procedimento civile che nel procedimento penale, i consulenti delle parti sono chiamati consulenti tecnici di parte (CTP).

Il perito è nominato dal giudice tra le persone iscritte negli albi professionali o tra le persone che hanno una particolare competenza nella specifica disciplina. Il perito è un pubblico ufficiale e ha l'obbligo di prestare il suo ufficio, salvo che ricorra uno dei motivi di astensione previsti dalla legge. Se il perito non è in grado di svolgere l'incarico, il giudice può nominare un altro perito. Il perito può essere anche nominato da una delle parti, ma in questo caso il perito è chiamato consulente tecnico di parte (CTP).

Il CTP può assistere al conferimento dell'incarico al perito e presentare al giudice richieste, osservazioni e riserve. Il CTP può partecipare alle operazioni peritali, proponendo al perito specifiche indagini e formulando osservazioni e riserve. Se il CTP è nominato dopo l'esaurimento delle operazioni peritali, può esaminare le relazioni e richiedere al giudice di essere autorizzato a esaminare la persona, la cosa e il luogo oggetto della perizia. L'attività dei consulenti tecnici non può ritardare l'esecuzione della perizia e il compimento delle altre attività processuali. Inoltre

- I consulenti tecnici devono essere imparziali e non possono avere interessi personali nella controversia.
- I consulenti tecnici devono essere competenti nella specifica disciplina oggetto della perizia.
- I consulenti tecnici devono svolgere la perizia con diligenza e professionalità.
- I consulenti tecnici devono redigere una relazione che contenga le conclusioni della perizia.
- Le conclusioni della perizia sono utilizzate dal giudice per decidere la controversia.

Dunque l'attività di consulenza ai fini giudiziari comporta una responsabilità disciplinare derivante dall'iscrizione all'ordine professionale cui normalmente afferisce e una responsabilità civile (art. 64 c.p.c.) che è una forma di responsabilità extracontrattuale da fatto illecito che può essere fatta valere solo nell'ipotesi in cui il consulente incorra in colpa grave nell'esecuzione dei suoi compiti.