RISPOSTE COMPUTER FORENSICS

Spiegare le fasi di

Individuazione

E' la fase dove si individuano i luoghi fisici e virtuali dove risiedono i dati informatici di rilevanza forense.
E' una fase molto importante perchè tutti quei luoghi non individuati, non potranno essere poi raccolti ed analizzati con conseguente perdita di valore forense.
I luoghi possono essere del più ampio ventaglio:dal computer all'automobile, il cellulare, tablet, ipod etc. In luoghi virtuali come il cloud. I tipi di dati sono vari: documenti, file multimediali, email, file di log etc. I social sono un altro luogo importante: facebook, instagram, instant chat etc.

Raccolta

Si vuole fare l'acquisizione del supporto di memorizzazione con la copia bit a bit, senza inquinare il reperto informatico ne in acquisizione ne in conservazione. Bisogna altresì garantire la catena di custiodia, con form per reperto oppure multi form cioè per i reperti di un intero caso; viene tracciato chi, quando, come dove e perché accede al reperto e altre informazioni tecniche. L'acquisizione non é copia incolla o altre sciocchezze ma è eseguita con specifici strumenti come: write blocker, write blocker usb, software licenziati che loggano in automatico tutte le operazioni fatte e calcolo hash, hardisk wipati. Ci può l'acq post mortem con il beneficio della staticità ma meno utile se fs criptato; acq live ha grande volatilità e più contestabilità ma con fs criptato può permettere facile accesso.

Analisi

Va condotta su delle copie mai sull'originale. Dobbiamo presentare dei risultati oggettivi, cioè dei dati, non delle valutazioni che possono cambiare in modo soggettivo. Dobbiamo rispondere alle 5W who, when, where, which,why; in aggiunta si deve rispondere anche: quante volte è successo e se c'era consapevolezza; possiamo rispondere leggendo specifici dati come, log, documenti, fotografie, metadati, coordinate gps etc etc. Poi ancora, si effettuano ricerche per autore, date, contenuto, tipo di file, hash, soggetto (email); ancora: recupero dati cancellati e carving; cracking di pw di documenti con dizionario, social engineering e brute force. Analisi artefatti sist.operativo. Si usa la timeline: una ricostruzione in ordine cronologico degli eventi costruiti con i metadati dei file di un filesystem di data di creazione, ultima lettura e scrittura. La supertimeline arricchisce la timeline con dati ottenuti dalle informazioni contenute in altri file come ad es. Il registro di windows.
A coda: ricerche con sinonimi, operatori booleani, regular expression e sintassi particolari; analisi su internet history, cache e cookies; analisi artefatti di windows: cestino, log eventi, registry, restore point, link, chiavette usb; su quest'ultime: marca, id dispositivo, data ultimo collegamento e altri metadati. Link analisys, consiste nella costruzione di un datawarehouse basato su dati di ogni genere: email, file, chat, documenti, dati di navigazione, luoghi, organizzazione, veicoli, droghe, etc; il sw è in grado di rilevare correlazioni che all'occhio umano sfuggirebbero, permettono la costruzione di un quadro sinottico per spiegare i collegamenti;

Analisi - Casi pratici

MAC, modified access created. Evento sentinella; Istogramma con picco di lettura, e in stessa data inserimento penna usb: condizione necessaria ma non sufficiente, possiamo parlare di compatibilità con un evento di copia massiva.
OSINT open source intelligence (facebook, siti internet)
Gli header di un'email possono contenere molti dati utili e importanti: gli ip dei server di passaggio, l'indirizzo mittente, il client di posta; tali dati però potrebbero essere stati eliminati a causa di configurazione dei server. Utilizzando tali informazioni può essere possibile risalire fino all'utenza telefonica; ci vogliono accertamenti per verificare tutte le ipotesi e possibilità; per es. nel caso ci siano 4 persone nell'appartamento, ci si dovrà accertare chi possa essere ragionevolmente l'autore originale e non dare per scontato che l'autore sia l'intestatario dell'utenza.

Valutazione

La valutazione è necessaria perché la prova informatica può essere (aic) alterata,inquinata, contraffatta; si deve verificare che le operazioni di acquisizione siano legittime. Il ct deve fornire seguenti dati sul reperto (aia) attendibilità, integrità e autenticità; in questo modo il giudice può esprimere una valutazione: attenzione il ct deve rimanere al proprio posto e fornire dati e non valutazioni. Se il bit è certo, perchè dobbiamo valutarlo? Camera:da letto,fotocamera,dei deputati! Vanno interpretati dal giudice grazie ai dati forniti dal ct. I sistemi informatici possono fornire errori, che complicano la valutazione; lo scenario di rete può rendere più difficile ma potrebbe fornire più dati. Scala di Casey (C0, contraddice i fatti, C7 sicuramente non contraffatta in virtù)

Presentazione

Viene stesa una relazione tecnica; con termini più semplici e divulgativi possibili con tante similitudini e metafore senza esagerare con terminologia tecnica. Deve essere comprensibile a non tecnici (come il giudice). La presentazione orale può presentare delle provocazioni dalle controparti a cui non si deve abboccare.

Network forensics: 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. Scopo è il monitoraggio e analisi del traffico di rete con origine o destinazione differenti computer o reti. Buona parte delle attività è costituita da

intercettazioni che quindi pongono gli elementi e i reperti in dubbio di liceità e utilizzabilità come prova. Le motivazioni sono per ingiurie, minacce a mezzo internet, pedopornografia, accesso non autorizzato ex 615ter cp, frodi

Domande da proporre sul forum

http://ssrionline.unimi.it/mod/forum/discuss.php?d=1889#p9637:

Si dia una definizione di informatica forense

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.

Informatica forense studia a **fini probatori** i processi, le tecniche e gli strumenti per l'esame metodologico dei sistemi informatici (memorie, hard disk, dischetti, nastri, cartaceo, etc.), nonché l'analisi forense di ogni sistema informatico e telematico (computer, rete di computer, ed ogni altro dispositivo per il trattamento di dati in formato digitale), l'esibizione della prova elettronica, l'esibizione del dato digitale, il recupero di dati e la loro esibizione, l'analisi ed esame del sistema informatico e telematico

Si illustri la rilevanza dell'adozione best practices nell'ambito dell'informatica forense

Quali sono le criticità dell'informatica forense?

Il reperto informatico è per sua natura volatile, facilmente modificabile, di facile contraffazione ed è difficile ricondurlo ai veri autori; da questo ne deriva la presunzione di ripudio.
E' importante avere un approccio metodologico (il CT è il chiodo non il martello) per essere pronti per la "prova di resistenza giudiziaria".
E' necessaria una profonda attività autocritica. Bisogna applicare una diffidenza quasi paranoica di fronte agli elementi riscontrati. Bisogna essere diffidenti: proprio quando vediamo un ipotesi confermata, è proprio il momento giusto per mettere nuovamente tutto in dubbio.
Il CT deve rimanere al proprio posto: non è un investigatore, non è un giurista e non è un giudice.

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

Individua univocamente in un preciso istante una utenza telefonica; infatti un utente ha intestato un'utenza e in un dato momento un indirizzo ip gli viene assegnato in modo univoco.
Attenzione però non sempre questa associazione è valida come nel caso di centraline accessibili e manomesse, doppini ricablati.

Quale deve essere il ruolo del consulente tecnico?

Il CT deve rimanere al proprio posto;non è un investigatore, non è un giurista, non è un giudice.
Assumerà il ruolo del "chiodo" in quanto le affermazioni, attività e conclusioni verranno passate alla "prova di resistenza giudiziaria"

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

L'ultimo accesso è la data di ultima lettura; ultima modifica è la data dell'ultima scrittura nel file.
Questo dato è facilmente manipolabile. Un modo è quello di modificare l'orologio del sistema.
Un altro modo è quello di utilizzare il tool touch che permette di manipolare questi dati molto facilmente.

http://ssrionline.unimi.it/mod/forum/discuss.php?d=1889#p17859:

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

dd if=/dev/zero of=/dev/sda

Scrivere l'espressione regolare che consente di individuare tutti i dati di codice fiscale italiano
[0-9]{16}
Oppure ([0-9]{4}\s?){4}

Scrivere l'espressione regolare che consente individuare tutti i dati di carta di credito (16 cifre)
[A-Z]{6}[0-9]{2}[A-Z][0-9]{2}[A-Z][0-9]{3}[A-Z]

Domande da compiti forse da NON proporre sul forum

Esame 2017-09-11

1) scrivere il comando linux per clonare l'hardisk hdd su hdg
Clonare: dd if=/dev/hdd of=/dev/hdg
Immagine: dd if=/dev/hdd of=/root/immagine.dd
Wipe: dd if=/dev/zero of=/dev/hdg
Immagine con errori: *dd if=/dev/sdb of=/media/sdc1/disco.dd conv=noerror,sync bs=32K*

2) cosa e' lo slack space che tipo di dati puo' contenere
Lo slack space e' lo spazio finale di settore non utilizzato dal file che ha allocato per ultimo quel settore
"I file quando sono salvati vengono allocati in cluster, gruppi di settori del disco, ma se un file occupa 5 cluster e mezzo, viene allocato in sei cluster, lasciano mezzo cluster libero."

3) Una persona vuole produrre come prova tre sms presenti nel suo cellulare. Descrivere dettagliatamente le operazione da condurre per diminuire la probabilita' di disconoscimento dalla controparte
Eliminare, alterare o creare ad arte sms è un'operazione molto semplice: ci sono software che permettono di farlo sia su dispositivi mobili recenti che vecchi. Consideriamo anche che ci sono servizi internet che per pochi euro permettono di spedire sms con numero telefonico mittente a piacere. Quindi per aumentare la resistenza della prova giuridica, dobbiamo dotarci di tutti gli elementi che possano aumentare l'efficacia delle argomentazioni, come: gli sms sia del dispositivo mittente che destinatario, i tabulati sia dell'sms in uscita che in entrata.
4) indicare i vantaggi della copia per immagine rispetto alla copia per clone
Una copia immagine è un file con tutti i vantaggi correlati: non abbiamo bisogno di un supporto uguale a quello originale, possiamo metterlo su un qualsiasi supporto con altri file immagine, possiamo comprimerlo senza perdita alcuna, potremmo anche spedirla senza ausilio di vettori fisici (per es. via internet), ci permette di creare una copia clone (è vero anche il contrario) ---vedere capitolo su virtualizzazione
5) Un'acquisizione di una pagina web ha md5 xxxxx. Il giorno dopo viene ripetuta l'acquisizione che ha hash md5 yyyy. Entrambi le acquisizioni fanno riferimento alla pagina www.sito.it/pagina.html. Spiegare come cio' sia possibile

6) Un'acquisizione post mortem di un hardisk ha hash md5 xxxx. Il giorno dopo viene ripetuta l'acquisizione post mortem e l'hash md5 e' yyyy. Entrambi le acquisizioni sono state fatte sullo stesso hardisk sorgente. Spiegare come cio' sia possibile
Ipotesi a) Se si intende l'hash compreso il log dell'acquisizione, allora viene inclusa anche la data dell'acquisizione stessa e quindi, quella del giorno successivo avrà una data differente e quindi un hash differente. Ipotesi b) L'acquisizione non è stata fatta con tutte le cautele possibili, per esempio senza un write blocker, quindi il disco collegato al sistema ha subito delle alterazioni (per esempio modifica ai metadati del filesystem,data di apertura filesystem, dirty bit) e questo ha portato ad un inquinamento del reperto e la seconda acquisizione avrà hash diverso. Ipotesi c) il disco aveva da sempre zone danneggiate e costretto quindi ad usare opzioni particolari (per esempio nel dd noerror,sync), tra la prima e la seconda acquisizione il disco ha subito un deperimento e gli errori sono aumentati.
7) Siete il CTP del sig X. Il Sig X ha scaricato del materiale pedo pornografico e da un sito web, il quale ha loggato il suo indirizzo ip come sorgente della richiesta. Quindi la prova della colpevolezza consiste nell'indirizzo ip emerso dalle indagini che e' stato assegnato all'utenza domestica assegnata al Sig x. Per l'accusa tanto basta per dimostrare che a scaricare il materiale pedopornografico sia stato il sig. x. Argomentare in difesa del proprio cliente
L'associazione dell'indirizzo ip all'utenza del Sig.X non è elemento probatorio sufficiente in quanto quel log potrebbe essere stato generato da altra causa che la deliberata volontà del Sig.X; quel log può essere stato generato da un malware oppure un trojan proxy. Ad ogni modo si richiede un accertamento tecnico mirato a verificare l'esistenza di effettive operazioni in software specifici di navigazione, che possano confermare o negare l'esistenza di azioni volontarie di download da parte del Sig.X

Chi me le ha date ha detto che sono di due esami; non ricorda esattamente quali di uno e quali dell'altro.

ecco le domande:
1) Com'è possibile capire ~~l'intestatario~~ (?) mittente di una mail? 1-2-6 vedi: analisi - casi pratici
~~2)Spiegare la fase di analisi~~
3) Descrivere due strumenti hardware per la disk forensics
Write blocker è uno strumento tra pc e disco sorgente, anche in versione per supporti usb come usb-pen o usb-disk; blocca i comandi di scrittura e accetta quelli di la lettura. Questo permette di acquisire una copia forense in tranquillità di non inquinare il reperto.
Copiatore hardware, ci si collega il disco origine e destinazione, permette la creazione di copia per immagine e clone e fare wiping, è molto veloce e comodo da trasportare per le ridotte dimensioni; esegue anche compressione dei dati.
~~4)Cos'è il wiping~~
5) Handover di confinamento e salvataggio, cos'è e fare un esempio
E' un'operazione che avviene ad un mobile station quando cambia BTS. Salvataggio quando il livello del segnale scende al di sotto di una certa soglie e quindi l'unità decide di spostarsi su un'altra BTS; questo può capitare quando siamo in viaggio. Confinamento quando la BTS è molto affollata e quindi il mobile device decide di passare su un'altra BTS magari anche più lontana e meno potente; questo può capitare in zone affollate come uno stadio.
6) Spiegare il metodo di acquisizione di una pagina web
1) utilizzo di una macchina virtuale con installato un sistema operativo Linux di tipo forense;
2) avvio di una procedura di registrazione audio e video delle operazioni eseguite, utili allo scopo di riprodurle in maniera "semplice" e comprensibile anche per un non tecnico;
3) avvio di una procedura di intercettazione del traffico di rete generato dalla macchina virtuale durante le attività di navigazione, utile per acquisire non solo i singoli file scaricati dal browser, ma anche le richieste e le risposte complete dai vari webserver contattati e per documentare in maniera inequivocabile gli indirizzi IP coinvolti;
4) consultazione di un sito dal quale poter documentare la data di inizio dell'acquisizione (ad esempio, l'homepage di un quotidiano online);
5) consultazione di tutte le pagine da acquisire utilizzando una procedure di consultazione manuale delle pagine di interesse o di strumenti per acquisizione di porzioni di sito in maniera automatica;
6) consultazione di un sito dal quale poter documentare la data di fine dell'acquisizione (ad esempio, l'homepage di un quotidiano online);
7) chiusura della procedura di intercettazione del traffico di rete; chiusura della procedura di registrazione audio e video;
8) spegnimento della macchina virtuale;
9) generazione di un archivio compresso contenente i file della macchina virtuale, il file della registrazione audio-video, il file di traffico di rete, i singoli file delle pagine web;
10) calcolo dell'hash dell'archivio compresso prodotto al punto precedente;
11) applicazione di marca temporale all'hash calcolato al punto precedente.fine. Il tutto deve inoltre essere dettagliatamente illustrato in una relazione tecnica che verrà allegata al fascicolo

~~7)Come si fa il wiping~~

Che differenza c'e' tra formattazione e wiping
La formattazione libera gli indici e rende disponibile lo spazio al sistema operativo ma non pulisce i settori dove risiedono i dati dei file; al contrario, il wiping permette una cancellazione completa, cioe' e' un'attivita' di scrittura di tutti i settori e quindi di tutta la superficie del disco.

Elementi di mobile forensics
I dispositivi mobili sono praticamente equivalenti al computer; hanno le stesse potenzialità, anzi di più. Il mobile è una fonte ricca di dati forensi: rubrica (con gruppi), registro chiamate, email, agenda, chat, client navigazione, navigatore etc. L'acquisizione logica: viene fatta via bluetooth, via cavo usb o dedicato o, per esempio via wifi. L'acquisizione fisica richiede specifici strumenti hardware e specifici strumenti per la comprensione. In estrema razio, acquisizione con agent, che però potrebbe essere contestato dalla controparte. Sempre in extrema ratio, acquisizione con fotografie o filmati.
La valutazione dell'attendibilità dei riscontri (mobile)
Gli sms sui dispositivi mobili sono di facile contraffazione e creazione. Ci sono dei software appositi che permettono la falsificazione completa dell'sms. Per replicare la procedura ci si dota di un dispositivo uguale per verificare quale sia la eventuale procedura di contraffazione. Ad ogni modo questo era già possibile con vecchi dispositivi nokia. Ci sono anche dei servizi di telefonia che possono falsificare il caller id e mittente sms. Quindi nell'accertare l'originalità e la genuinità di certi elementi bisogna tenere conto di quanto detto e si devono utilizzare tutti le fonti a disposizione quali: sms del dispositivo di invio rispetto al dispositivo di arrivo, i tabulati telefonici.
La geolocalizzazione dei dispositivi di telefonia mobile
I dispositivi di telefonia mobili MS, sono identificati univocamente dall'international mobile equipment identity (IMEI), usano una Subscriber Identity Module (SIM) e si collegano alla base transceiver stations (BTS). L'handover è il processo

di passaggio di utilizzo da una BTS ad un'altra. La linea di un handover ideale è una retta equidistante dalle due antenne. Nella pratica, causa variabilità del segnale delle BTS l'handover deve essere rilevato direttamente sul campo con dei dispositivi di rilevazione di potenza del segnale. La documentazione del traffico ha valore indiziario, viste queste variabilità: deve poi essere rinfrancato da elementi di riscontro (scontrini, passaggi telepass, multe…)

8)è possibile usare la stampa di una pagina web come prova in un processo?
Non c'è un divieto ma sarebbe un tentativo goffo e disperato perchè non supererebbe la prova di resistenza giudiziaria. Le stampe, fax, print screen di pagine web etc non sono valide prove perchè non possono ...
9)Elencare 1 tool per tipo per cercare parole chiave, traffico di rete e per dispositivi mobili
Ricerca veloce su parole chiave: FTK forensics toolkit. Traffico di rete: wireshark. Dispositivi mobili: Oxygen forensics (e IEA)
10)Descrivere bts, mobile station, imei e imsi (international mobile subscriber identity)

11)Come si acquisisce un dispositivo mobile senza tool?

12)A cosa serve la catena di custodia e quali tipi ci sono?
Serve per conservare la storia del o dei reperti informatici. Viene scritto chi, dove, quando accede al reperto, data e ora del sequestro ; sono anche presenti il digest,i dettagli tecnici e i dati di produzione di fabbrica del reperto. Può essere single-evidence: solo per un reperto; multi-evidence: per i reperti relativi ad un singolo caso. 1-2-3-alla fine
13)A cosa serve l'immagine di windows in fase di processo
Può essere usata per mostrare degli esperimenti; tali operazioni si possono ripetere tutte le volte necessarie, visto che si parte da una copia dell'immagine e quindi l'oggetto di partenza sarà sempre lo stesso.

Esperimenti, resuscitare la macchina, malware testare comportamento, non si altera il reperto originale, si può ripetere, ausilio nella spiegazione di metodi e risultati per es. in dibattimento al giudice, pm, avvocati. Sempre pronta per ripetere operazioni analoghe come acquisizioni di pagine web. Macchine con tool precaricati per analisi. Virtualizzazione di un'immagine forense (VBoxManage convertdd /mnt/img.dd /mnt/img.vdi, xmount, liveview) e poi hash

Da facebook: domande: qualcuna sui comandi linux, definizione informatica forense, come si effettua copia forense hd, qualcuna sul mobile forensics....cmq per la maggiore domande di teoria

TIMELINE SUPERTIMELINE

Viscosità dei dati si intende la caratteristica dei dati informatici di rimanere "aggrappati" al supporto informatico e dunque alla difficoltà di far sparire qualsiasi traccia di un dato. In altri termini, nell'ambito del normale trattamento di un sistema informatico da parte di un utente, i dati tendono a rimanere in più punti (si pensi al file di word che genera tanti file temporanei, può avere tracce nella memoria virtuale...) e laddove venissero cancellati possono permanere comunque sotto altre forme (ad esempio, nello slack space). Proprio in considerazione dell'elevata probabilità di trovare dati "abbandonati" e dati per distrutti, l'acquisizione forense deve essere completa perché consente il recupero di informazioni anche molto vecchio e rimaste nel supporto

File system un caso reale 2-1-2 Fase di destruens e construens

Marcatura temporale: utile quando si opera da soli, la si fa solo sull'hash e non su tutto il contenuto. Si può acquistare alla stregua dei francobolli in tabaccheria. Un modo alternativo semplice e gratuito è inviare a se stessi una pec.

Embedded forensics: la criticità è la grande eterogeneità dei dispositivi, cito alcuni ambiti: automobilistico, sanitario, antinfortunistico, industriale. E' importante quindi mantenere un rigoroso rispetto dei principi forensi ed effettuare una scrupolosa documentazione e per una corretta acquisizione. La sperimentazione, per quanto possibile, è uno strumento fondamentale per portare la miglior forma di verifica che possa superare la prova giudiziaria.

Analisi - strumenti software
Autopsy: disk forensics gratuito, legge vari fs, recupero file cancellati, carving. E' più lento delle controparti commerciali; fornisce un'ottima timeline.
EnCase: vari fs, timeline accurata, linguaggio scripting per automazione, preview file multimediali.
Internet Evidence Analyzer: ricerca tutte le evidenze di attività fatte, chat, navigazioni, documenti, dropbox, gdrive, email, webmail (e documenti consultati), analisi copia di backup disp. Mobile; analisi attività programmi file sharing; analisi social network; altre analisi su browsers.

FTK forensic toolkit ricerca di più parole chiave, velocità molto elevata nella ricerca grazie a pre indicizzazione; analisi fs, carving e anteprima documenti; formati raw,SMART,e01,aff
Oxygen Forensics analisi dispositivi mobili, analisi di copie di backup di disp.mobili, cronologia messaggi, multimedia e timeline e supertimeline con locazioni gps.
P2C Paraben Commander analisi di database (pst,edb) di email di grandi dimensioni e export in eml.
Nirsoft vari tool gratuiti, lista dispositivi usb
Guymager esporta in fari formati, può fare una rilettura di controllo e verifica dell'acquisizione.