Mi sono svegliato tardi quindi mi mancano i primi 20 minuti

Durante questi venti minuti parla principalmente dell’introduzione con definizione di alibi(non-presenza, presenza fisica o scusanti che attestino di non avere fatto un reato, reato in un luogo diverso), l’alibi informatico è teoricamente facilmente contraffabile, è molto semplice fare un alibi informatico.

Tecniche di antiforensics

Riscontri oggettivi per cui l’indagato si trovava in un posto diverso rispetto al delitto, è una giustificazione , se è totalmente attestato l’indagato viene totalmente scagionato dall’investigazione.

Trovarsi in un altro luogo, sia virtuale in modo da non aver compiuto il diritto, che fisico per non essere nel luogo del delitto(sempre se ha un luogo ben definito)

Come già detto nella scorsa lezione, da parte della difesa basta mettere il dubbio, se l’alibi non è totalmente errato, allora non si ha la certezza della colpevolezza dell’indagato o degli imputati

Durante le indagini bisogna comunque considerare come può essere stato costruito un alibi, in modo da vedere se sia reale o fittizio-costruito.

I tabulati del traffico di dati vengono chiesti alle autorità giudiziarie

Ci sono molti modi di simulare un alibi, si possono usare app di connessione e controllo remoto tramite software, oppure si possono utilizzare dei programmi che simulano l’utilizzo del computer.

Cosa ci da la sicurezza che colui che ha fatto le azioni che costruiscono l’alibi sia effettivamente il proprietario delle credenziali(complici, bot, script)

Si potrebbe creare inoltre delle prove ex novo prima o dopo l’evento.

Per smontare questi alibi potremo vedere possiamo cercare queste evidenze descritte qui sopra(script, programmi,accessi a team viewer, traffico ed altro)

Un perito o un consulente tecnico deve fare sempre tutto in buona fede, se sbaglia ci può stare, ma se mente di propria volontà o perché costretto è penalmente conseguibile

È possibile risalire agli spostamenti del soggetto anche da celle telefoniche, non solo dal gps, anche se è abbastanza più difficile

Per creare questi automatismi, esistono inoltre molti modi di renderli indistinguibili da altri automatismi.

Non è necessario essere un hacker per creare automatismi e per creare questi alibi informatici fittizzi, esistono inoltre applicazione che simulano questi automatismi

Una esercitazione opzionale entro il 15 aprile: creare ad-hoc un falso alibi informatico su un dato device e un dato SO

DIFFAMAZIONE IN RETE

Reato punibile penalmente da 6 mesi a 3 anni di reclusione.

Il reato(l’insulto) non deve essere fatto di persona(ingiuria),indiretto, l’insulto sia destinato al determinato oggetto,

sindrome dell’abitacolo su internet(leoni da tastiera), perdita di molti freni inibitori.

Altri reati su internet sono infiniti(revenge porn, rilascio di informazioni confidenziali, etc…)

La cassazione ha riconosciuto il reato di diffamazione commesso via internet.

Querela fatta da un utente offeso(che ritiene), l’importante è fare subito la acquisizione prima che il presunto diffamatore cancelli il messaggio-diffamazione.

Diffamazione sulla base di onore, riservatezza e identità personale,(accanto a reputazione)

L’insulto non deve essere diretto, basta che sia deducibile l’obiettivo per esclusione(il figlio minore del dottore sono io)

Noi ci occupiamo di ambito penale, ma possiamo comunque utilizzare le nostre conoscenze per l’ambito civile per risarcimenti di denaro

Documentare la presenza di diffamazione:

la stampa in pdf o su carta non viene solitamente ammessa in tribunale perché non gode dell’integrità(?)

2)notaio: certificazione di un notaio o di un pubblico ufficiale, alternativa migliore ma non è solitamente sufficiente(sempre usare le best practices in modo che l’acquisizione sia inattaccabile)

EX facebook: identificazione del profilo, utilizzare il codice univoco(?) id della singola pagina-profilo, questo id sarà lo stesso indipendente dal cambio di nome del profilo o altro. Inoltre si è più precisi nella richiesta dei dati del profilo a facebook

Allo stesso modo, si può creare una pagina che attesti la colpevolezza ma sarebbe fittizia, quindi bisogna dimostrare che online non c’è la controparte reale.

Post con attivazione delle notifiche, congelarlo come boh.

OSINT(open source intelligence), come attività di raccolta di informazioni mediante la consultazione(da rivedere)