**Social network**

Oggi è l’ultima lezione prima della pausa, si rientra a lezione il 20

Ci sarà una prova in itinere con test a risposta multipla (potrebbero essere anche a risposta aperta ma chi se ne frega)

La prima parte di questa prova avrà a che fare con i social network forensics, in particolare identificazione e acquisizione dei dati utili per l’indagine, analizzare tre social da quella lista di social, il post diffamatorio è univoco, il post è acquisibile, come faccio a risalire agli autori, ed ai commentatori, vengono identificati gli utenti, alcuni di questi social potrebbero essere privati, insomma tutte le caratteristiche utili per l’indagine.

Devo fare il numero 6,106,206 entro il 10 aprile (facebook, asmallworld, telegram)

La seconda parte sarà il giorno 9 aprile dalle 8:30 alle 9:30, risposta multipla

**Posta elettronica**

Resta comunque uno dei modi più usato per comunicazione formale.

Ovviamente la comunicazione è asincrona, i messaggi vengono recapitati ai server degli appositi destinatari, nell’attesa di essere letti, il vantaggio della posta elettronica è di avere un recapito teoricamente sempre attivo

Tramite telnet è possibile inviare messaggi da server email di altri propietari ad altri umani(spoofed email), dai log è possibile vedere che il messaggio è stato inviato tramite telnet

L’intestazione contiene molti dati utili

MIME per cose diverse oltre il testo, anche formati multimediali

L’analisi della posta può essere fatta i in remoto sul server, o nel client

Nei client c’è una opzione che mostra gli header.

Tool:email tracker per vedere il percorso delle mail

Una parte cruciale della analisi è l’identificazione dell’utente

DKIM firma digitale che stabilisce che i gestori di un dominio firmato abbiano applicato la firma certificando il contenuto e le intestazioni del messaggio (poco usato), garantisce la spedizione da quel dominio

Fake mail creabile facilmente

La firma elettronica manca nelle mail semplici

Il valore giuridico della mail resta tale finché non viene ripudiata-disconosciuta, la mail non ha alcun valore legale se viene disconosciuta, articolo 2712 c.c.

Se si vuole autenticare una mail bisogna utilizzare la firma elettronica semplice

Il giudice in generale può considerare l’email come prova, comunque si deve tenere conto delle caratteristiche di sicurezza della mail, sempre.

Un altro tipo di posta elettronica utilizzata per messaggi firmati è la PEC(post elettr certificata), molto simile alla raccomandata con ricevuta di ritorno, il mittente è garantito, il destinatario non può ripudiare, tracciamento univoco dei messaggi mandati e ricevuti

TOOLS nelle slide