Recap ultima lezione, perquisizione e inspezione, perquisizione come ottenimento del corpo del reato, a sorpresa, inspezione come ricerca delle prove digitali nelle prove ottenute durante la perquisizione.

**SEMINARIO INTRODUZIONE DI DISK FORENSICS**

È interessante, quindi me lo ascolto.

Si parla di disk forensics perché un tempo erano principalmente dischi, ma al giorno ci sono un sacco di hardware di memorizzazione (mass storage devices).

Avremmo un approccio top-down per trovare gli exploit.

Riconoscere i dispositivi non è semplice per la varietà di dispositivi.

-CPU reset per reinizializzare la CPU

-POST per vedere direttamente dall’elettronica se tutto sta andando bene

-BIOS come firmware che inizia a fare operazioni varie sul dispositivo, non possiamo sapere se sia stato modificato per distruggere tutto, bisogna evitare di accendere il dispositivo.

-BOOT

Cancellare o evitare la BIOS password, un metodo è distruggerla resettando il BIOS

Evitare di utilizzare il sistema operativo, non si sa come gestisce i dati e come sia stato cambiato.

Il dato come già visto ha più rappresentazioni dipendenti dalla architettura interna, Little o Big endian.

Windows si fa fregare dalle estensioni dei file, non sulla base del magic number, linux invece controlla direttamente il magic number.

Log files vari, registri di sistema di windows, /var/log di linux, etc…

Le informazioni dello SMART sono talmente generali che non servono poi cosi a tanto.

Sistemi operativi live-USB come best practice per garantire la write block e le funzionalità sono esattamente quelle dichiarate(CAINE top bellezza da quel che ho visto, penso che anche SIFT sia buono)

Guimager e autopsy sono semplici e forniscono la maggiorparte dei tool necessari per analisi e acquisizione, per analisi più complesse bisogna andare nello specifico.