ORDINE AVVOCATI TORINO  COMMISSIONE SCIENTIFICA

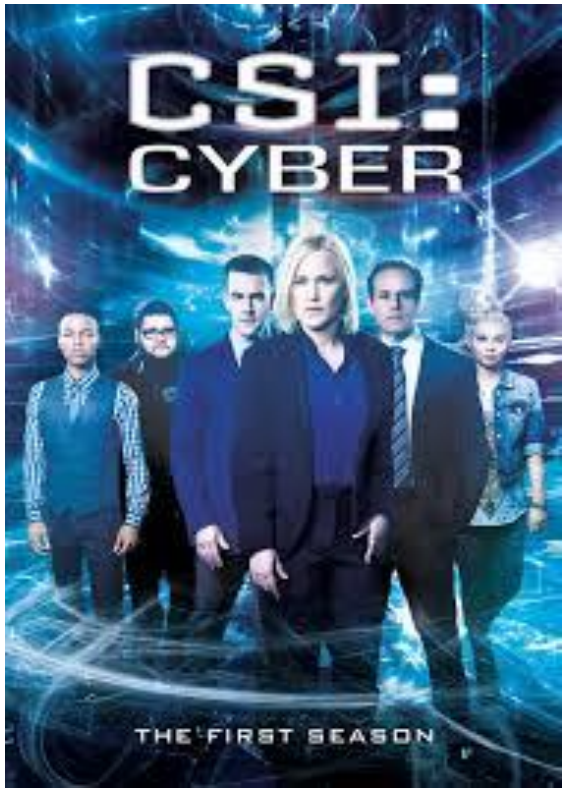
21 NOVEMBRE 2019

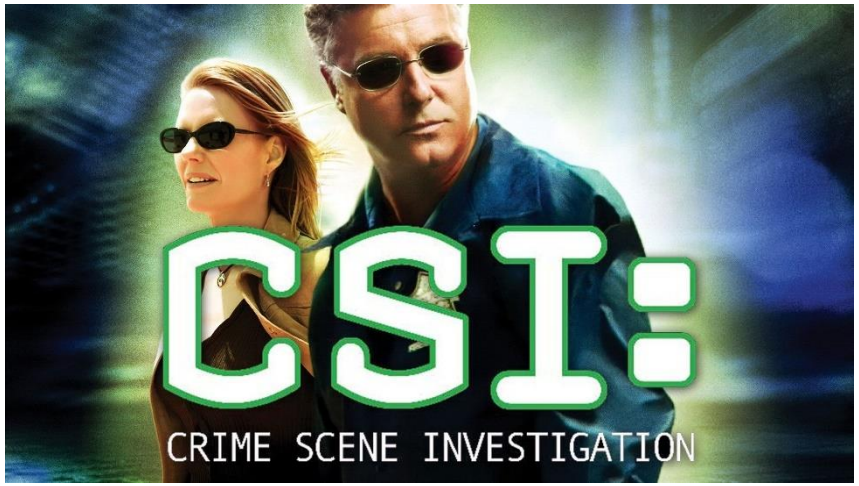
LO STRUMENTO INFORMATICO QUALE MEZZO PER LA COMMISSIONE DEL REATO

L'acquisizione degli elementi di prova digitali: dalla copia forense alla copia logica di «server» e dispositivi mobili, gli strumenti a disposizione degli investigatori per la ricerca dei dati, problematiche, soluzioni e limiti

I sequestri di materiale informatico e le indagini forensi

COSA NON E' LA DF





COSA NON E’ LA DF

- **TUTTI SANNO USARE QUALSIASI SOFTWARE ANCHE SE E’ LA PRIMA VOLTA CHE LO VEDONO**
- **I VIRUS SONO IN 3D E LA LORO GRAFICA E’ MIGLIORE DELLA PLAYSTATION 4**
- **I VIRUS TI PARLANO E TI AVVISANO CHE STANNO PER DISTRUGGERE IL COMPUTER. DOPODICHE’ IL PC FA LE SCINTILLE**
- **NESSUNO USA IL MOUSE MA TUTTI SCRIVONO SU TASTIERA ALLA VELOCITA’ DELLA LUCE**
- **PER AGGIRARE UNA PROTEZIONE BASTA SCRIVERE «BYPASS PASSWORD» IN UNA FINESTRA NERA CON IL CURSORE**
- **I PC DI QUALSIASI UFFICIO HANNO UN SOFTWARE CHE TI FA VEDERE IN 3D LA PIANTA DEL PALAZZO E DOVE TI TROVI**
- **SI PUO’ INGRANDIRE UN’IMMAGINE FINO A VEDERNE I MINIMI PARTICOLARI E NON SGRANA MAI. SE MAI SUCCEDE C’E’ UN BOTTONE MAGICO CHE RICOSTRUISCE LA FOTO**
- **PER TRASFERIRE DECINE DI MILIONI DI EURO BASTA PREMERE UN TASTO SUL CELLULARE E LA TRANSAZIONE AVVIENE IN TEMPO REALE E VEDI I SOLDI CHE AUMENTANO CON UN CONTATORE. TANTO FIGURATI SE LA BANCA TI CHIAMA PER CHIEDERTI COSA STAI FACENDO.**

VEDIAMO INVECE CHE COSA E' LA DIGITAL FORENSICS

L'informatica forense è la scienza che studia, in ambito giuridico:

l'identificazione

la conservazione

la protezione

l'estrazione

l'impiego

del dato informatico all'interno di un processo penale

L’ACCERTAMENTO FORENSE SUI DATI DIGITALI

- IDENTIFICAZIONE: individuare tutte le possibili fonti che possono contenere dati digitali in quanto gli stessi potrebbero essere facilmente nascosti sia dal punto di vista fisico che dal punto di vista logico.


4GB
micro SD


MEMORY STICK PRO DUO

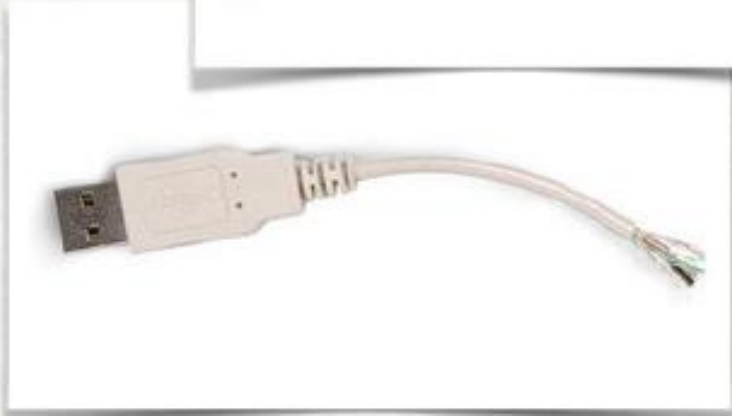

Nikon
COOLPIX


87.5


Life in Luxury


TE QUIERO


Kierunek piątek.




SONY
10:35


4LIVE
London
0.35
TOMTOM

L’ACCERTAMENTO FORENSE SUI DATI DIGITALI

ACQUISIZIONE

Le copie dei dati DEVONO essere identiche all’originale (cd copia bit to bit)

la garanzia di conformità all’originale ci viene data dagli algoritmi di HASH

Nel linguaggio matematico e informatico, l'hash è una funzione non iniettiva (e quindi non invertibile) che mappa una stringa di lunghezza arbitraria in una stringa di lunghezza predefinita. Esistono numerosi algoritmi che realizzano funzioni hash con particolari proprietà che dipendono dall'applicazione.

TUTTE LE PROCEDURE DEVONO ESSERE BEN DOCUMENTATE E ATTUATE UTILIZZANDO METODI E TECNOLOGIE CONOSCIUTE IN MODO DATALE CHE SIANO VERIFICABILI DALLE CONTROPARTI

L’ACCERTAMENTO FORENSE SUI DATI DIGITALI

PRESERVAZIONE

Il Reperto Originale NON deve essere alterato

UTILIZZO DI WRITE BLOCKER

UTILIZZO DI DISTRO FORENSI COME CAINE O DEFT

PREVIEW:

L’ACCERTAMENTO FORENSE SUI DATI DIGITALI

ANALISI – ESTRAZIONE - IMPIEGO

recuperare i dati e «lavorarli» per ricostruire informazioni utili attraverso l’utilizzo di software dedicati

interpretare i dati per verificarne l’utilità nell’ambito delle indagini rendendoli utilizzabili dalla PG operante

CONVENZIONE DI BUDAPEST
Legge 48/2008

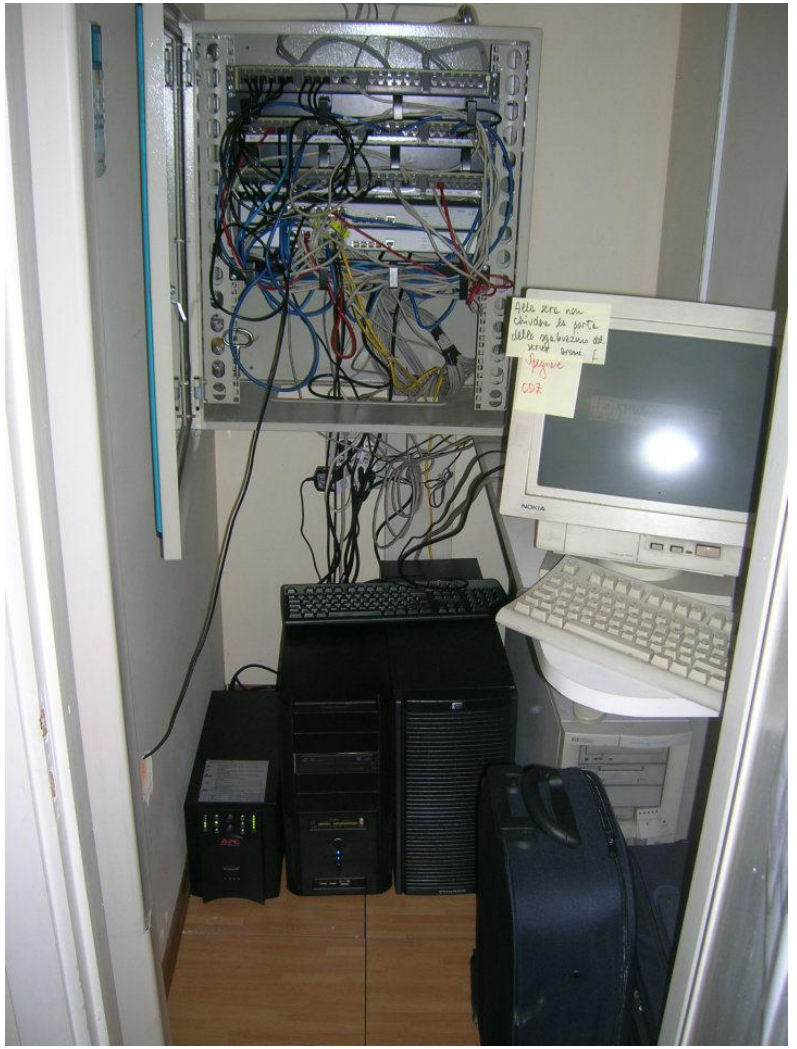
OGGI

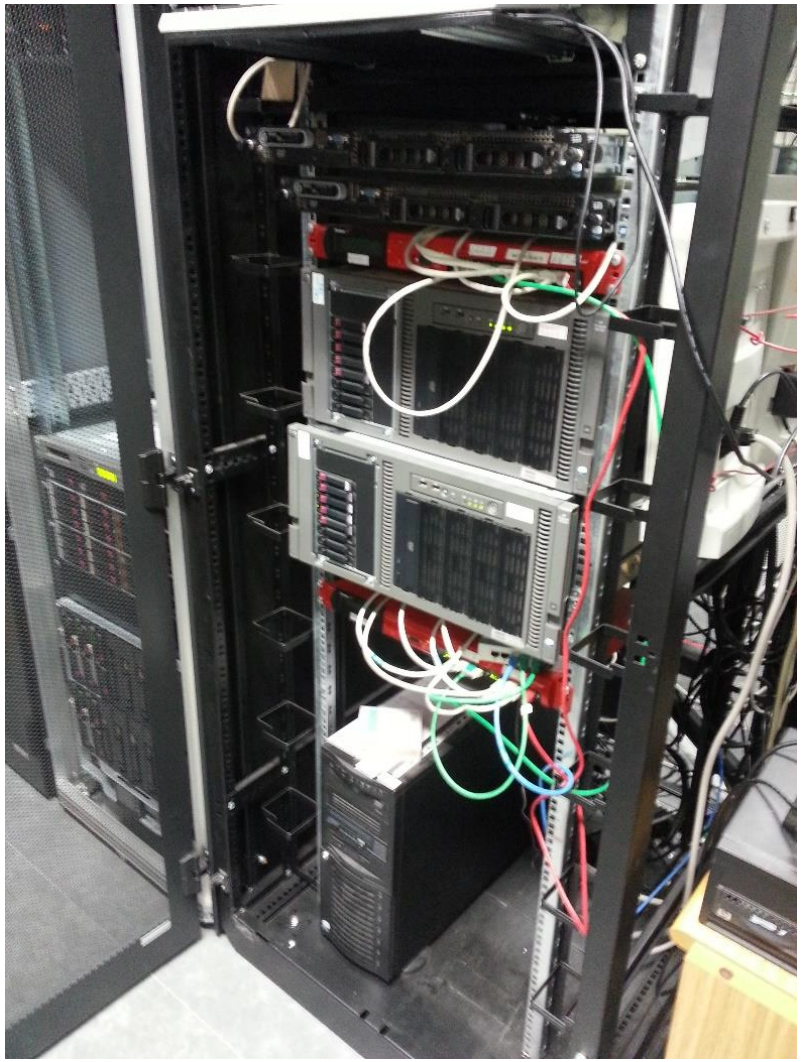
VS

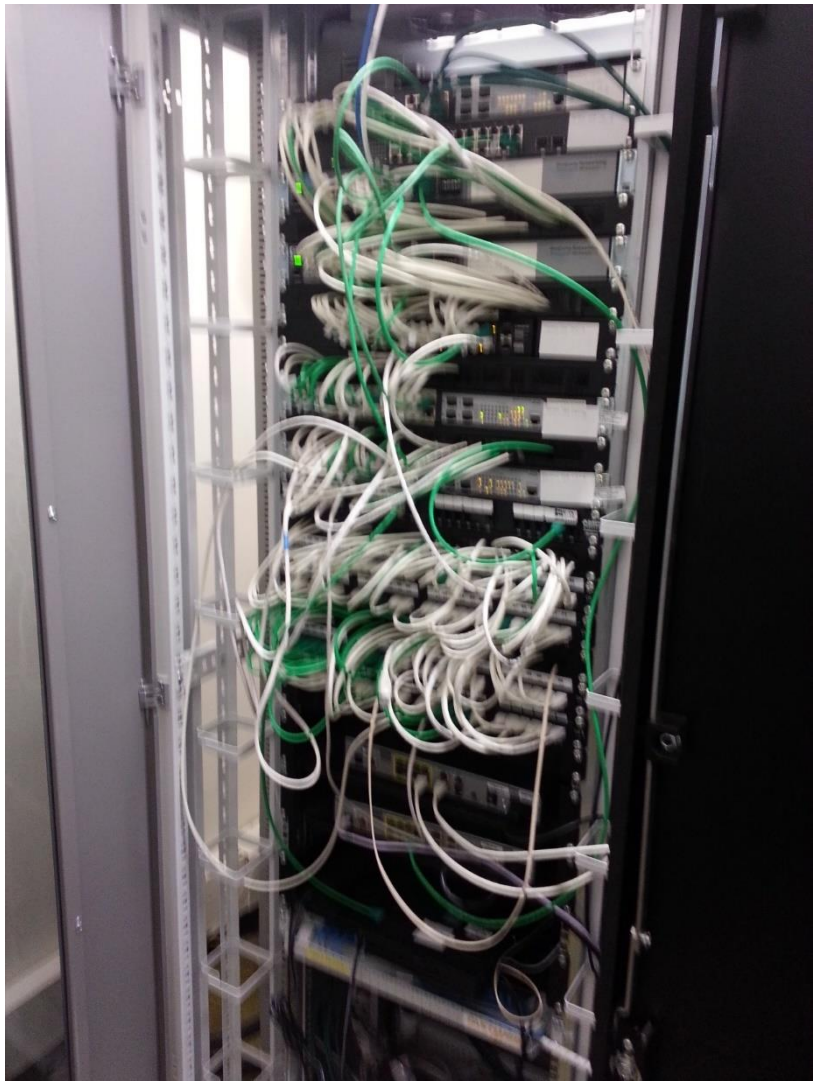
ESEMPI DI ATTIVITA' SVOLTE DALLA SEZIONE INFORMATICA FORENSE

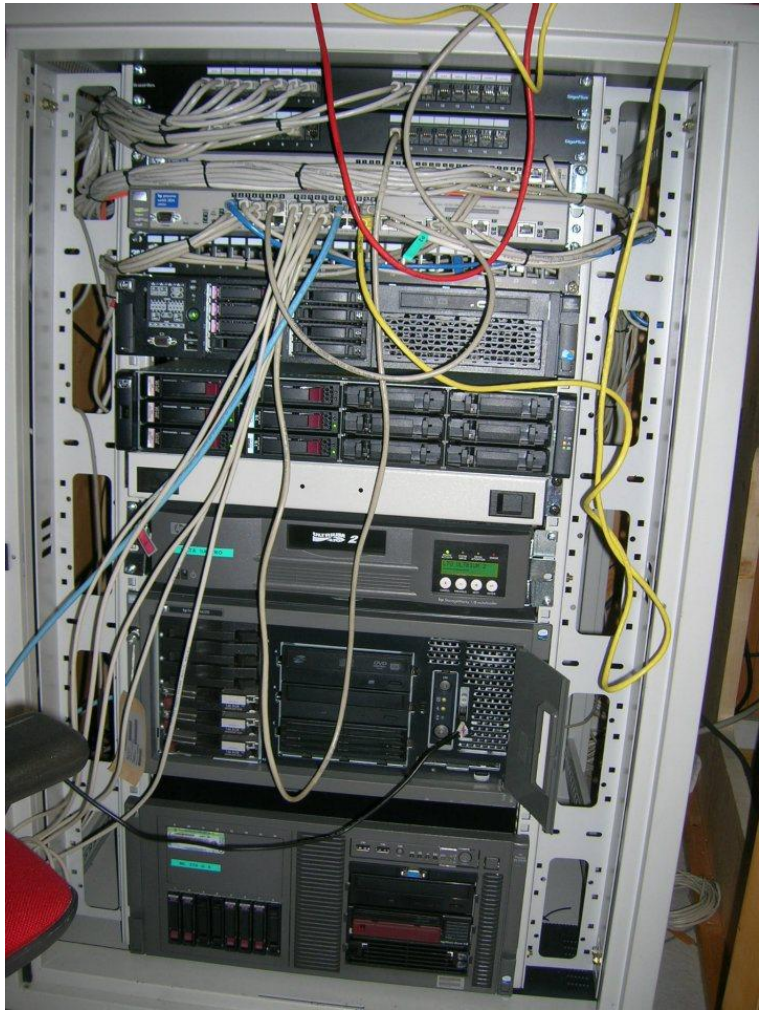
- Professionista
- P.M.I
- Grande realtà

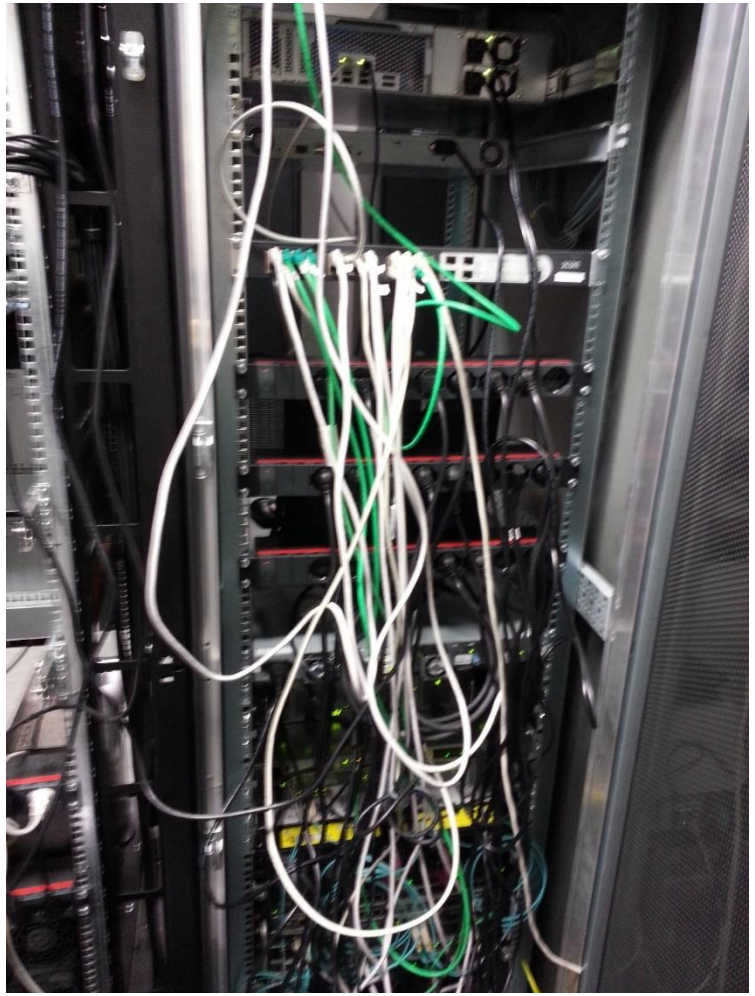

STABLEAU


Alle ore non chiudere la porta della mansarda ed avvisare
Grazie
CDZ









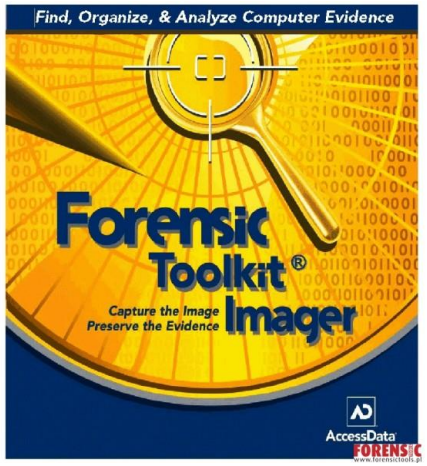
Dopo aver valutato lo scenario operativo è necessario:

- **Concordare con la PG operante quali siano gli obiettivi**
- **Valutare i passi necessari per lo svolgimento dell'attività**
- **Valutare il tempo a disposizione che può influenzare le scelte operative**

SCEGLIERE GLI STRUMENTI PIU’ ADATTI

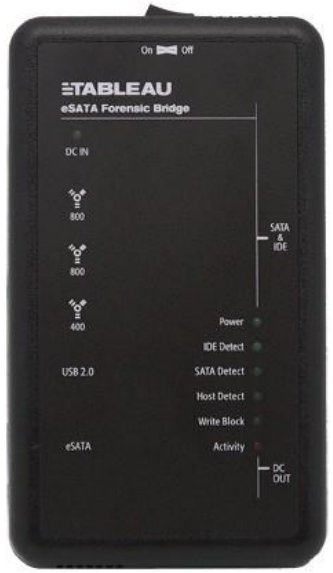
SCEGLIERE GLI STRUMENTI PIU' ADATTI

Software OpenSource



SCEGLIERE GLI STRUMENTI PIU’ ADATTI

Dispositivi Hardware



Esecuzione dell’acquisizione «forense»:

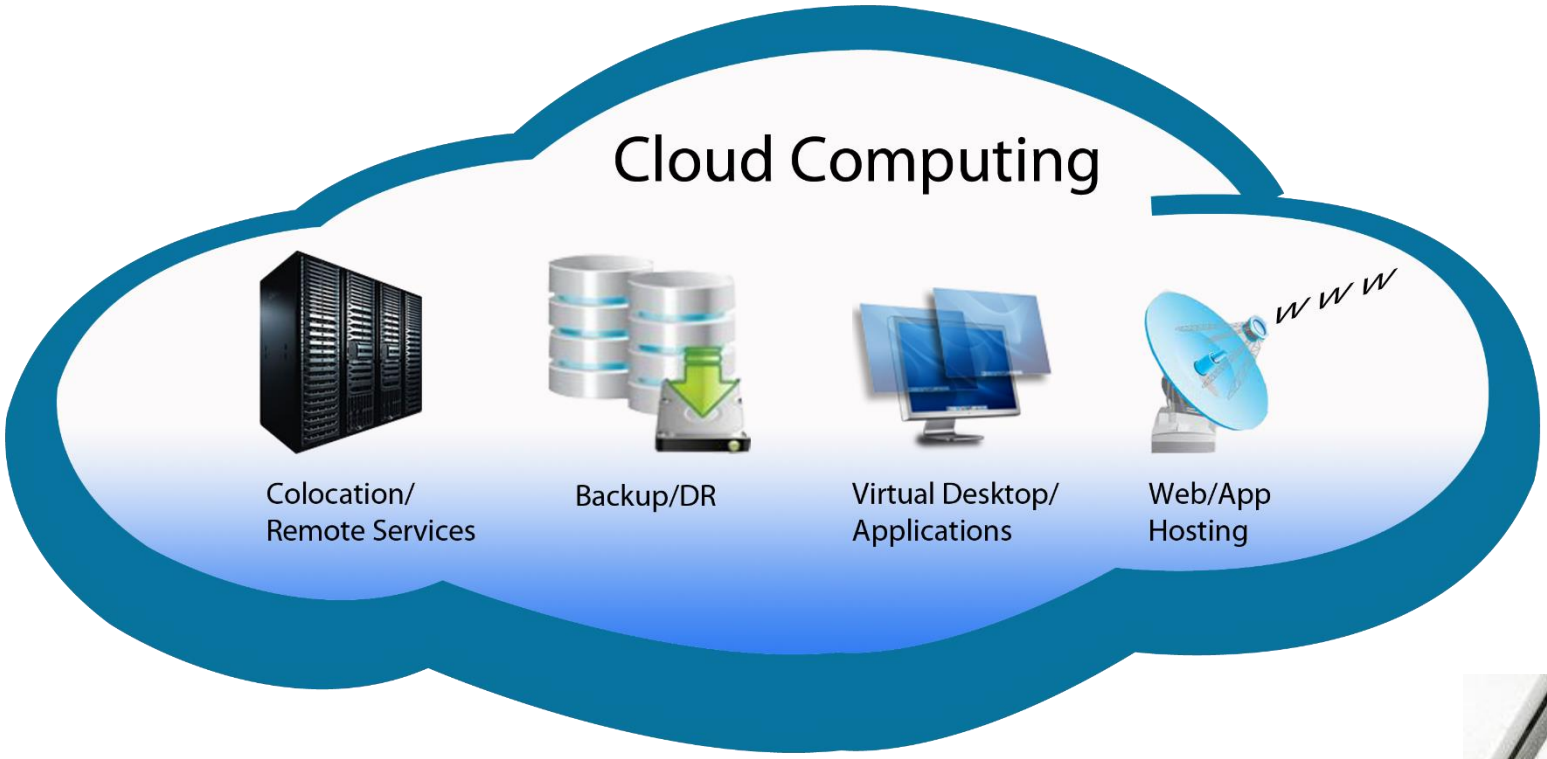
A LIVELLO PIU’ BASSO POSSIBILE IN FUNZIONE DEL DEVICE O DEL SUPPORTO CHE ABBIAMO DI FRONTE

- **Singole postazioni (client)**
- **Server**
- **NAS**
- **Sistemi di Virtualizzazione**
- **Librerie a nastro magnetico (LTO)**
- **Sistemi di videosorveglianza**

METODOLOGIA INVESTIGATIVA

DETERMINAZIONE DEI RISCHI

- **Copertura data dal decreto di perquisizione**
- **Perquisizione informatica o Ispezione** (*quando vi è fondato motivo di ritenere che dati, informazioni, programmi informatici o tracce comunque pertinenti al reato si trovino in un sistema informatico o telematico, ancorché protetto da misure di sicurezza, ne è disposta la perquisizione, adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione*" **)**
- **Assistenza del personale IT aziendale (intero o esterno) – Ausiliario di PG**
- **Presenza dell'indagato/parta assistito dal difensore.**


Cloud Computing
Colocation/
Remote Services
Backup/DR
Virtual Desktop/
Applications
Web/App
Hosting
www


save to cloud

SISTEMI CLOUD

INSIEME DI RISORSE HARDWARE E SOFTWARE UTILIZZABILI E ACCESSIBILI DA REMOTO

SISTEMI CLOUD

USI MOLTEPLICI

- **Storage** (Skydrive – Gdrive - Dropbox – Googlemaps – Flickr – Youtube)
- **SaaS Software as a Service** (Webmail – Google Docs)
- **PaaS Platform as a Service** (Facebook – Windows Azure – Amazon Web Service)
- **Iaas Infrastucrute as a Service** (Amazon EC2)

SISTEMI CLOUD

DIFFICOLTA' INVESTIGATIVE

- I sistemi cloud sono «normalmente» distanti dal luogo dell'intervento. A volte anche all'estero. (es servizi google per le aziende)
- Interi sistemi possono essere spostati da un luogo ad un altro con un «click»
- Difficoltà di individuazione della risorsa remota
- Più Provider, più sistemi in paesi diversi
- Limiti legislativi
- Scarsità di accordi internazionali

SISTEMI CLOUD

COSA POSSIAMO FARE???

- navighiamo a vista tra le nuvole -

- Art 254cpp (*L'autorità giudiziaria, quando dispone il sequestro, presso i fornitori di servizi informatici, telematici o di telecomunicazioni, dei dati da questi detenuti, compresi quelli di traffico o di ubicazione, può stabilire, per esigenze legate alla regolare fornitura dei medesimi servizi, che la loro acquisizione avvenga mediante copia di essi su adeguato supporto, con una procedura che assicuri la conformità dei dati acquisiti a quelli originali e la loro immodificabilità. In questo caso è, comunque, ordinato al fornitore dei servizi di conservare e proteggere adeguatamente i dati originali*) Sequestro tramite inibizione account????
- Accesso ai sistemi con credenziali «fornite» dall'utente
- Verifica della presenza di applicazioni client (dropbox – gdrive – mega)
- Intercettazione telematica (captatore o spyware) – **problematiche legislative**

SISTEMI CLOUD

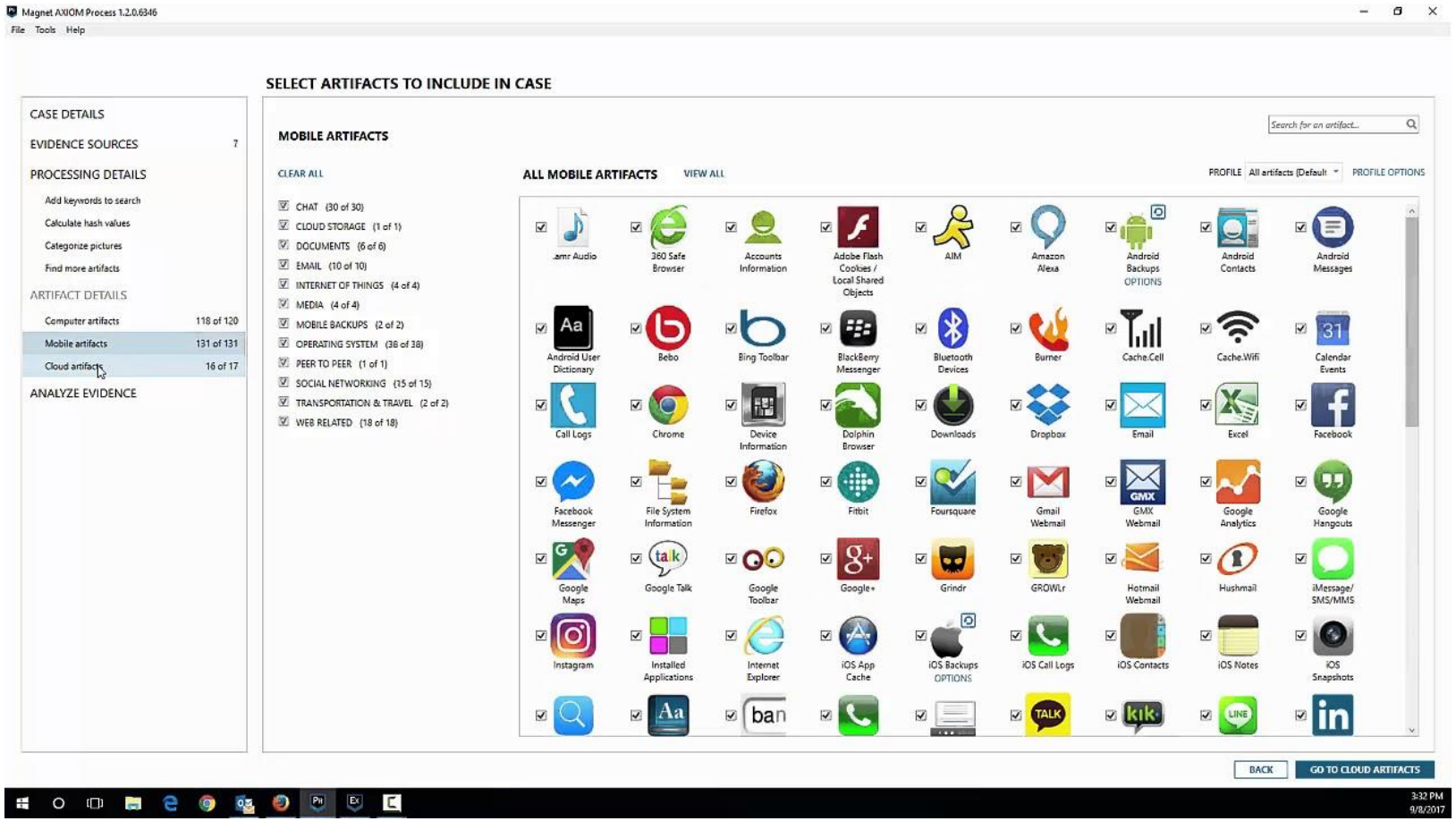
QUALSIASI PERCORSO OPERATIVO SCEGLIATE
LA PRIMA REGOLA DELLA FORENSIC AZIENDALE E’:

CERTIFICAZIONE E VERIFICA DI INTEGRITA’ DEL DATO ORIGINALE

STRUMENTI PER L'ANALISI DEI DATI

STRUMENTI PER L'ANALISI DEI DATI

MAGNET AXIOM™



ANALISI DI DISPOSITIVI MOBILI

Ragioniamo in funzione del dispositivo che ci troviamo di fronte (telefono tradizionale, smartphone o tablet)

La prima cosa da fare è quella di **chiedere immediatamente i PIN / Password di protezione. ATTENZIONE il PIN della Sim non è la stessa cosa del codice di protezione/blocco (particolarità su iphone – password bck iTunes)**

Verificata la correttezza dei codici spegnere il dispositivo o metterlo in modalità aereo

ANALISI DI DISPOSITIVI MOBILI

ATTENZIONE

Alle APP di controllo remoto

Alla possibilità di effettuare il «factory reset» da remoto.

STRUMENTI PER L'ANALISI DEI DISPOSITIVI MOBILI

STRUMENTI PER L'ANALISI DEI DISPOSITIVI MOBILI

ANALISI DI DISPOSITIVI MOBILI

Dispositivi Android:

Su molti modelli è possibile bypassare la protezione con la gesture di sblocco.

Molto difficile eludere il pin o la password (tentativi errati possono bloccare il telefono e renderlo inaccessibile)

I modelli di ultima generazione sono INACCESSIBILI se non si conosce il pin o la password di sblocco

ANALISI DI DISPOSITIVI MOBILI

Dispositivi iOS:

Il bypass del codice di blocco è possibile solo fino al iphone 4 o ipad 1

Per i modelli successivi si possono effettuare dei tentativi di sblocco ma dipende dalla versione dell'iOS instalalto.

CELLEBRITE C.A.S.

ANALISI DI DISPOSITIVI MOBILI

COSA SI PUO' FARE:

- Acquisizione di tipo Logico

L'acquisizione logica consisten in una copia dei files e delle cartelle che risiedono nella memoria del dispositivo. In questo tipo di copia il programma comunica con il dispositivo richiedendo le informazioni attraverso il sistema operativo nello stesso modo con cui operano i programmi per la sincronizzazione dei dati con un PC come ad esempio Nokia PC Suite.

Questo tipo di estrazione normalmente non consente di recuperare i dati cancellati.

ANALISI DI DISPOSITIVI MOBILI

COSA SI PUO' FARE:

- Acquisizione File System

L'acquisizione è molto simile a quella di tipo logico ma, in questo caso vengono acquisiti tutti i file e le cartelle presenti nel dispositivo e la loro intera struttura.
In questo caso per determinate applicazioni è possibile recuperare anche dati «cancellati» poiché quanto i dati sono salvati in database tipo SQLite, quando il dato viene cancellato, esso non viene sovrascritto ma solo marcato come "cancellato", permettendo in questo modo il recupero, fino all'eventuale sovrascrittura.

ANALISI DI DISPOSITIVI MOBILI

COSA SI PUO’ FARE:

- Acquisizione Fisica

L’acquisizione fisica di fatto è la copia bit-for-bit del chip di memoria del dispositivo. Operazione analoga alla copia forense di un hard disk

L’analisi dei dati acquisiti attraverso questa modalità permette quasi sempre il recupero dei dati cancellati.

ANALISI DI DISPOSITIVI MOBILI

COSA SI PUO’ FARE:

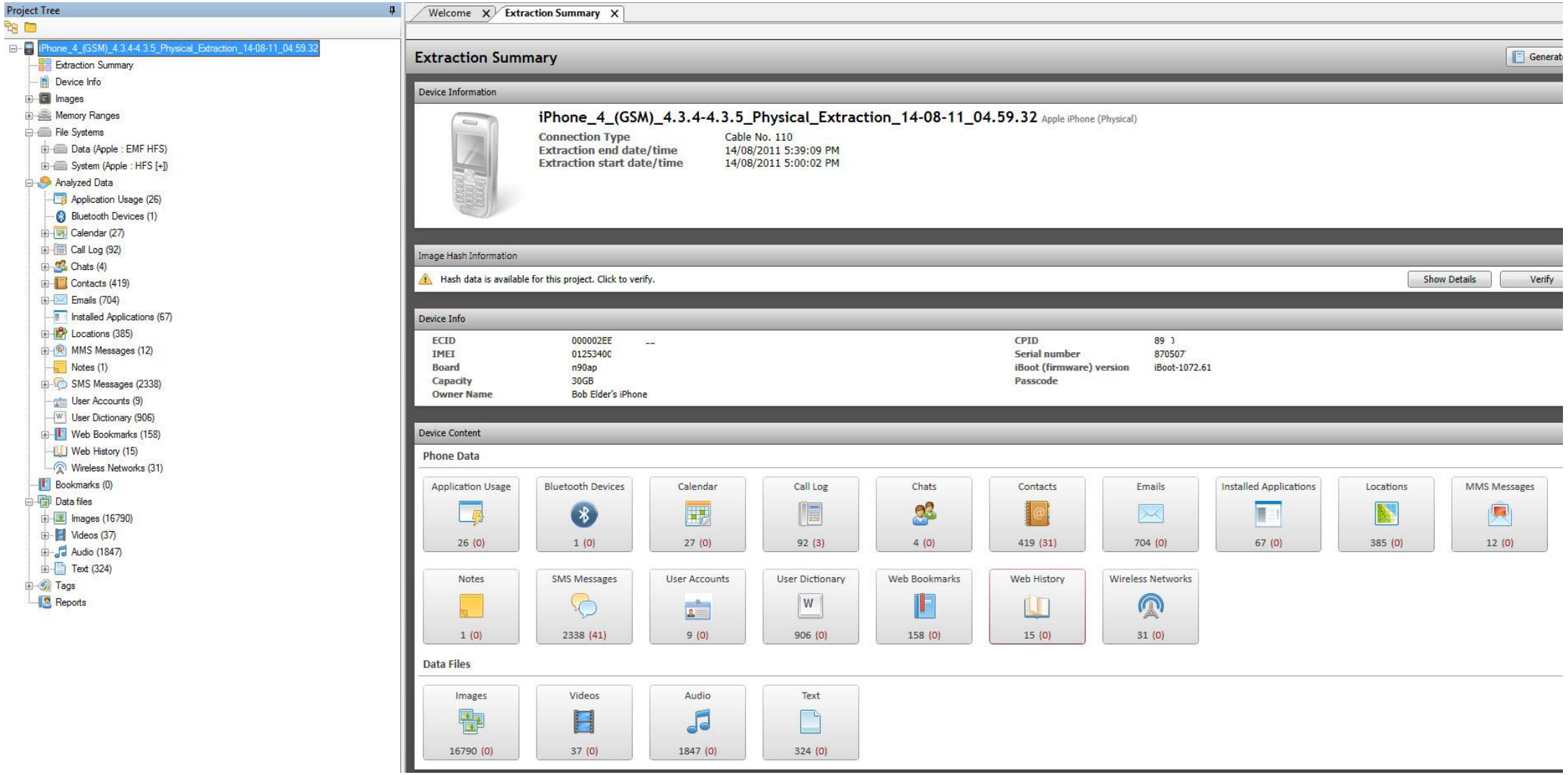
- Chip Off

Si tratta di un vero e proprio disassemblaggio del dispositivo mobile. Viene rimosso il Chip di memoria che viene letto attraverso degli strumenti esterni.

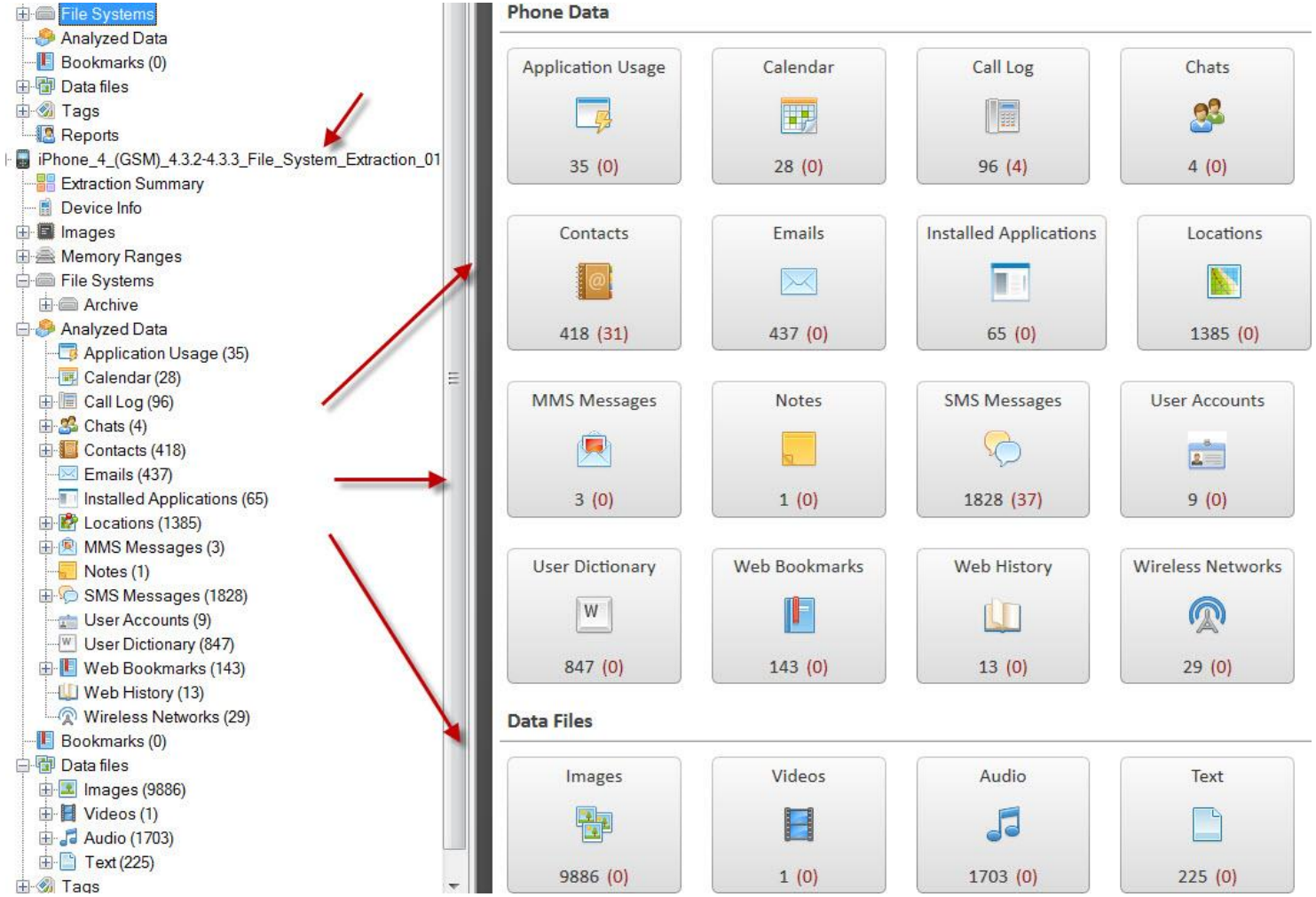
Questa operazione non è valida per tutti i modelli di telefono in quanto sempre più spesso i dati contenuti nei chip di memoria sono a loro volta cifrati pertanto anche dopo la loro acquisizione risulterebbero illeggibili.

ANALISI DI DISPOSITIVI MOBILI
caso particolare

STRUMENTI PER L'ANALISI DEI DISPOSITIVI MOBILI



STRUMENTI PER L'ANALISI DEI DISPOSITIVI MOBILI



GRAZIE PER L'ATTENZIONE

ANDREA PELLEGRINI

+39 0114327307

+39 3346468042

andrea.pellegrini@giustizia.it

Pellegrini.andrea2@gdf.it

CONTATTI

ANDREA PELLEGRINI

+39 0114327307

+39 3346468042

andrea.pellegrini@giustizia.it

Pellegrini.andrea2@gdf.it