Intercettazioni telefoniche e telematiche

Peculiarità tecniche e investigative

Agenda

- Introduzione del tema
- Intercettazione telefonica
- Intercettazione telematica
- Captatore telematico

Viviamo nell’era digitale

La maggior parte degli individui vive **immerso in un mondo digitale**, un mondo in cui i confini tra la vita online e quella offline si dissolvono all’ombra della **iper-connettività**.

cit. Luciano Floridi

botnet

chat

social network

game

messaggistica

blog

Come e dove «***comunichiamo***»?

smart tv

telefono

e-mail

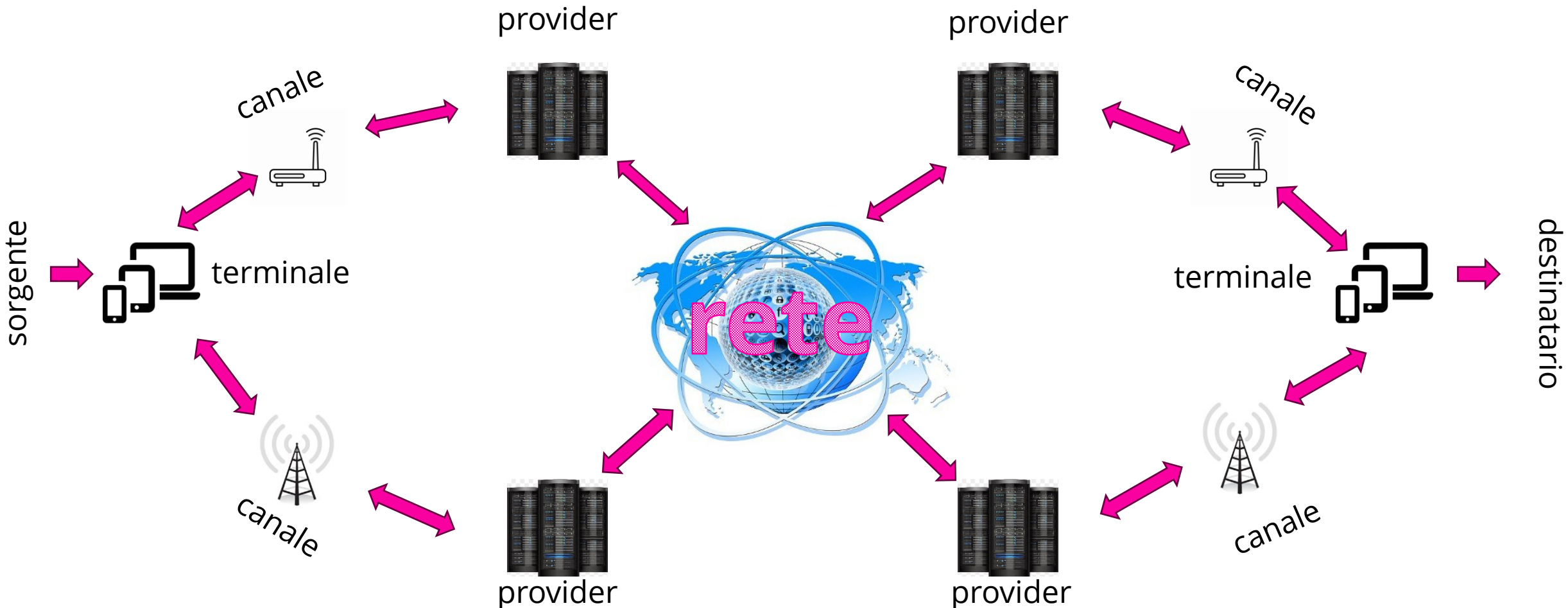
app

sms

video conference

Captare la voce e i dati

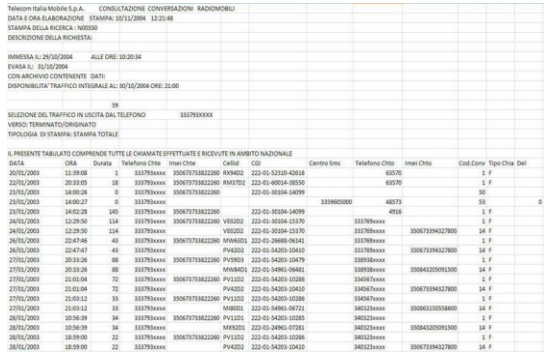
+ Tutte le comunicazioni a distanza si schematizzano in questo grafo



Cosa possiamo ottenere

Traffico sottoforma di tabulato

+ Mittente (numero utenza, apparato)
+ Ricevente (numero utenza, apparato)
+ Data e ora - Durata
+ Tipo comunicazione
+ Numero byte
+ Localizzazione / distanza



Telecom Italia Mobile S.p.A. CONSULTAZIONE CONVERSAZIONI RADIOMOBILI
DATA E ORA ELABORAZIONE STAMPA: 10/11/2004 12:21:48
STAMPA DELLA RICERCA : N00550
DESCRIZIONE DELLA RICHIESTA:

IMMESSA IL: 29/10/2004 ALLE ORE: 10:20:34
EVASA IL: 31/10/2004
CON ARCHIVIO CONTENENTE DATI:
DISPONIBILITA' TRAFFICO INTEGRALE AL: 30/10/2004 ORE: 21:00

39

SELEZIONE DEL TRAFFICO IN USCITA DAL TELEFONO 333793XXXX
VERSO: TERMINATO/ORIGINATO
TIPOLOGIA DI STAMPA: STAMPA TOTALE

IL PRESENTE TABULATO COMPRENDE TUTTE LE CHIAMATE EFFETTUATE E RICEVUTE IN AMBITO NAZIONALE

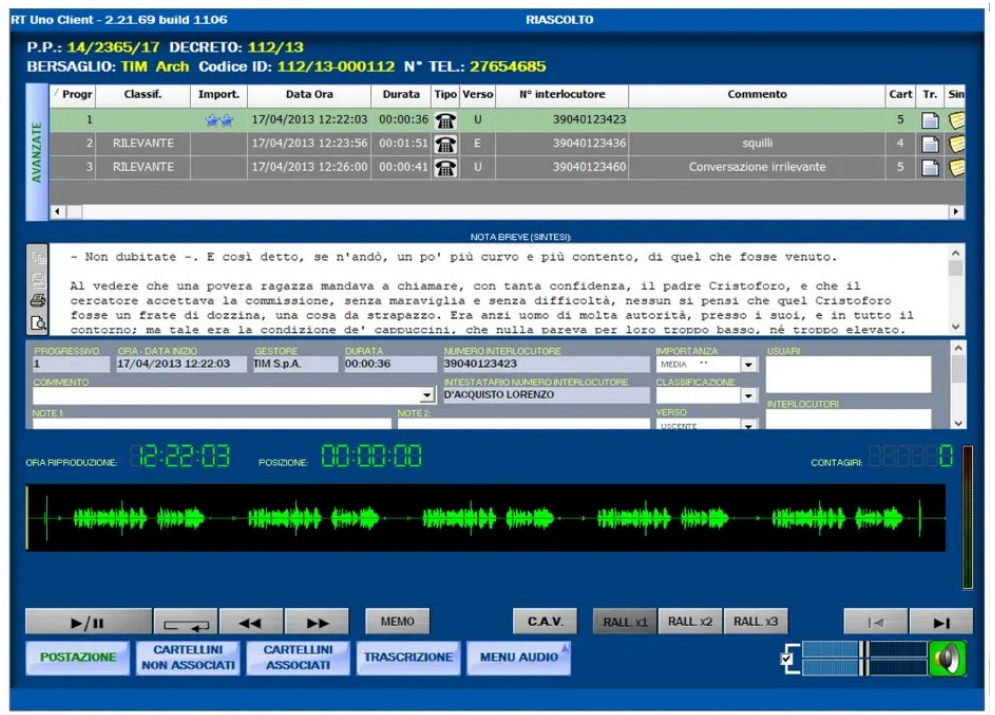
DATA	ORA	Durata	Telefono Chte	Imei Chte	Cellid	CGI	Centro Sms	Telefono Chto	Imei Chto	Cod.Conv	Tipo Chia	Del
20/01/2003	11:39:08	1	333793xxxx	350675733822260	RX9402	222-01-52310-42618		63570		1	F	
22/01/2003	20:33:05	18	333793xxxx	350675733822260	RM3T02	222-01-60014-38550		63570		1	F	
23/01/2003	14:00:26	0	333793xxxx	350675733822260		222-01-30104-14099				50		
23/01/2003	14:00:27	0	333793xxxx				3359605000	48573		53		0
23/01/2003	14:02:28	145	333793xxxx	350675733822260		222-01-30104-14099		4916		1	F	
24/01/2003	12:29:50	114	333793xxxx	350675733822260	YE0202	222-01-30104-15370		333769xxxx		1	F	
24/01/2003	12:29:50	114	333793xxxx		YE0202	222-01-30104-15370		333769xxxx	350673194327800	14	F	
26/01/2003	22:47:46	43	333793xxxx	350675733822260	MW6ID1	222-01-26688-06141		333769xxxx		1	F	
26/01/2003	22:47:47	43	333793xxxx		PV4202	222-01-54203-10410		333769xxxx	350673194327800	14	F	
27/01/2003	20:33:26	88	333793xxxx	350675733822260	PV5903	222-01-54203-10479		333938xxxx		1	F	
27/01/2003	20:33:26	88	333793xxxx		MWB4D1	222-01-54961-06481		333938xxxx	350843250591500	14	F	
27/01/2003	21:01:04	72	333793xxxx	350675733822260	PV1102	222-01-54203-10286		334567xxxx		1	F	
27/01/2003	21:01:04	72	333793xxxx		PV4202	222-01-54203-10410		334567xxxx	350673194327800	14	F	
27/01/2003	21:03:12	33	333793xxxx	350675733822260	PV1102	222-01-54203-10286		334567xxxx		1	F	
27/01/2003	21:03:12	33	333793xxxx		MIB0D1	222-01-54961-06721		340323xxxx	350866115055860	14	F	
28/01/2003	10:56:39	34	333793xxxx	350675733822260	PV1101	222-01-54203-10285		340323xxxx		1	F	
28/01/2003	10:56:39	34	333793xxxx		MX92D1	222-01-24961-07281		340323xxxx	350843250591500	14	F	
28/01/2003	18:59:00	22	333793xxxx	350675733822260	PV1102	222-01-54203-10286		340323xxxx		1	F	
28/01/2003	18:59:00	22	333793xxxx		PV4202	222-01-54203-10410		340323xxxx	350673194327800	14	F	

Contenuto della comunicazione

+ Voce
+ Testo
+ Immagini
+ Video
+ Metadati
+ Byte trasmessi
+ Protocollo di comunicazione
+ Software utilizzato
+ Date e ora - durata

Dove avviene l'intercettazione

- Il dato è prelevato direttamente dal provider e dirottato verso i server della Procura
  - Tabulati: telefonici o telematici
  - Contenuto: audio, testo, byte
- Dove viene memorizzato?
  Sui server della Procura (ADI)
- Distinguere il dato telefonico (*voce, sms, video*) e il dato telematico (*dati in chiaro e cifrato*)
- Sul dato intercettato deve essere apposto un sigillo digitale per garantire l'originalità e l'immodificabilità del conteruto



Criticità

- Le intercettazioni possono essere non intellegibili:
  - Molte comunicazioni avvengono tramite protocolli internet
  - Quasi tutte le comunicazioni utilizzano **protocolli cifrati**
  - Le comunicazioni sono spesso volatili
  - Le comunicazioni possono **one-to-one** (alcune app di messaggistica)
  - Le comunicazioni transitano su **server esteri**
  - Altre comunicazioni avvengono su piattaforme (social, mail, web conference, blog, app, ecc.)
- Metodi alternativi:
  - Captatore informatico
  - Copia forense del dispositivo
  - Copia forense dalla piattaforma

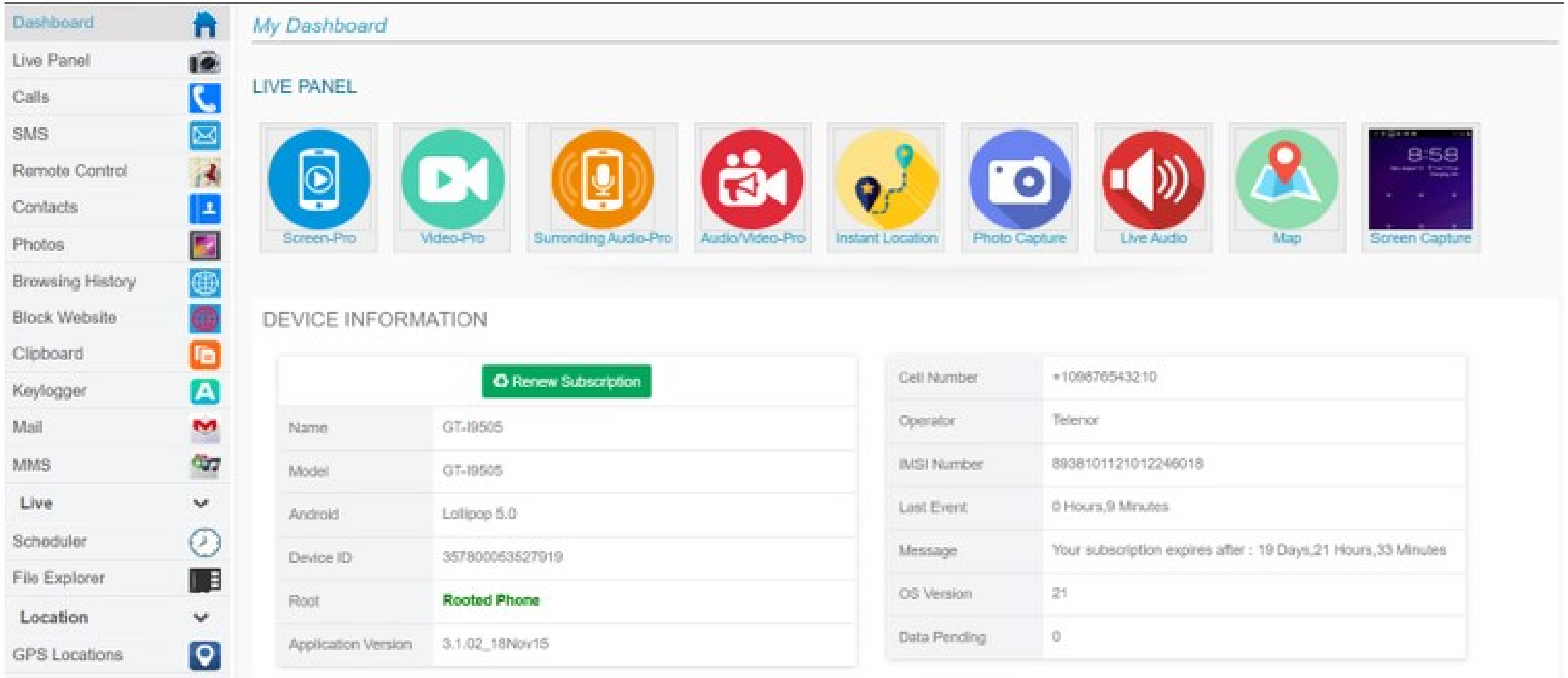
Captatore informatico

- Il captatore informatico è un RAT (Remote Access Trojan/Remote Administration Tool), un software che costituisce, per le forze dell'ordine e la magistratura (???), uno strumento per **controllare un dispositivo da remoto e bypassare i sistemi di cifratura delle comunicazioni**
- È tipicamente in grado di **acquisire** e/o **intercettare** le informazioni e le comunicazioni direttamente sul dispositivo acceso (online e offline) in maniera silente
- Viene iniettato negli smartphone e nei personal computer e, in base alle norme in vigore, può attivare il microfono per **ascoltare** le conversazioni, **geolocalizzare** il dispositivo, attivare la telecamera per **scattare foto o registrare video**, **leggere e copiare il contenuto della memoria**, **registrare** ciò che viene digitato, **intercettare** e **registrare** tutte le comunicazione e le attività effettuate dall'utilizzatore del dispositivo (quanti articoli del c.p.p. dovremmo citare?)
- **Tutte le attività poste in essere dall'operatore, dall'installazione alla disattivazione del captatore, le captazioni e le acquisizione, devono essere registrate e visionabili**
- **I dati devono transitare sui server della Procura**

Captatore informatico

+ L’inoculazione del captatore può avvenire principalmente in due modalità:
  - **da locale**: occorre avere la disponibilità del dispositivo e, quindi, viene installato il software direttamente dall’Autorità giudiziaria che dispone le intercettazioni. Oppure, occorre far avere un dispositivo preconfigurato all’origine, da fornire alla persona intercettata. Questa metodologia era più diffusa nel passato, mentre oggi si preferisce tentare l’inoculazione;
  - **da remoto**: tramite l’utilizzo di alcuni escamotages, la persona intercettata viene guidata ad installare sul proprio dispositivo il software che poi prenderà il controllo del dispositivo intercettato.
+ L’installazione può avvenire tramite l’uso di tecniche di hacking:
  - **Invio di email o messaggi**
  - **Sfruttamento di bugs tipo 0-day o exploit noti**
  - **Installazioni tramite download o aggiornamenti (provider)**
  - **Tecniche di social engineering**
+ Dopo l’installazione del captatore l’apparato ospite è:
  - **Alterato**: subisce un aggiornamento e non può essere ripristinato allo stato iniziale
  - **Vulnerabile**: il captatore abbassa i sistemi di sicurezza del dispositivo e blocca gli aggiornamenti di sicurezza
  - **Compromesso**: non è facile rimuovere il captatore e può essere riutilizzato

Captatore informatico

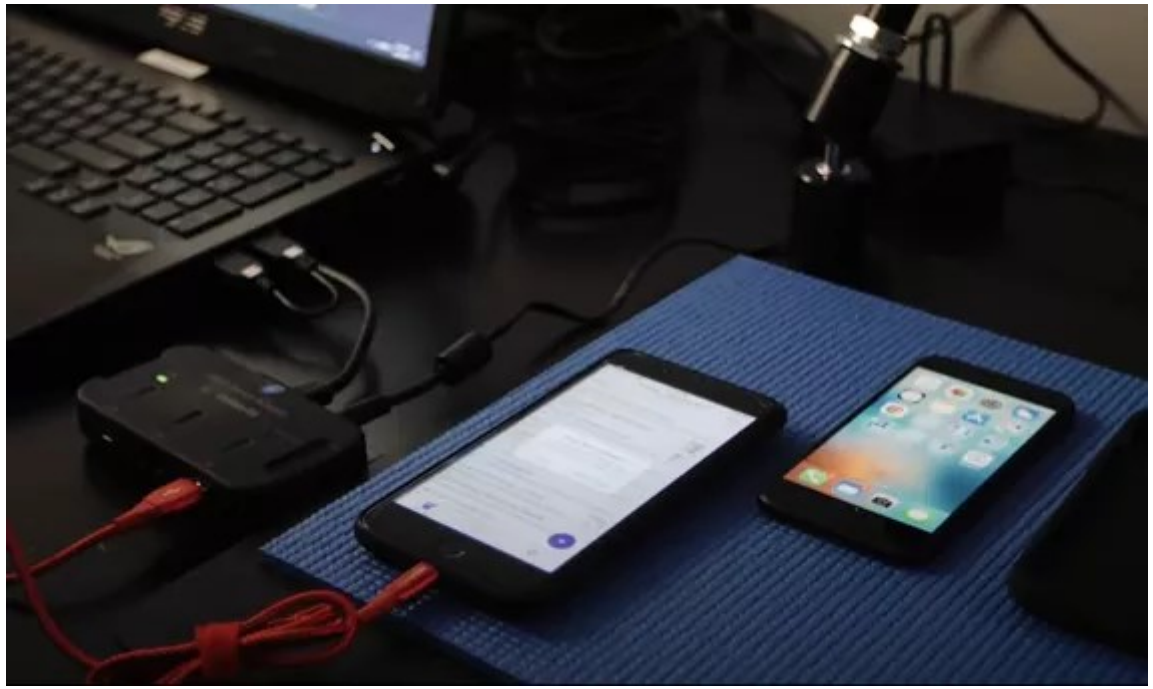


Acquisizione forense

- Come prescrive la norma (*Legge n. 48/2008*):
  - Le copie forensi devono essere **identiche** o il più possibile simili all'originale (in tal caso occorre giustificare la scelta)
  - Durante la copia dell'origine, quest'ultima **non deve essere modificata** (integrità)
  - Nel caso in cui non ci sia un metodo che consenta di evitare di alterare l'originale, la scelta va giustificata e documentata
  - Le procedure devono essere attuate e documentate secondo metodologie e tecnologie riconosciute, in modo da poter **essere verificabili** dagli altri attori (verificabilità)
  - Potrebbe essere necessario eseguire copie parziali della memoria del dispositivo, anche in questo caso la scelta deve essere motivata e documentata

Metodologia

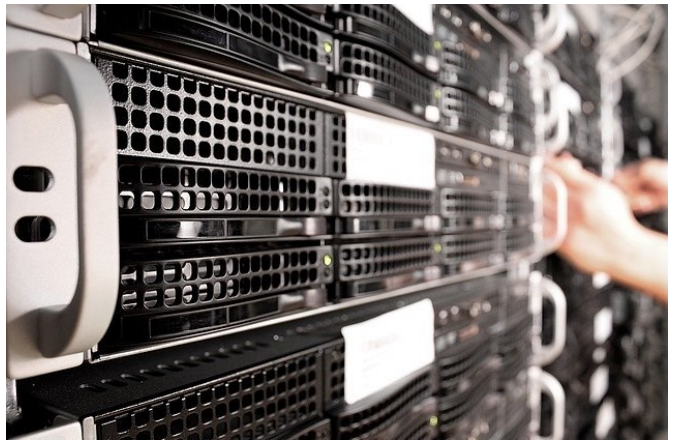
- La ISO/IEC 27037:2012 "*Guidelines for identification, collection, acquisition, and preservation of digital evidence*«, diventata lo standard de facto, fornisce le linee guida relative alla gestione delle potenziali prove digitali, concentrandosi in particolar modo sulle fasi di **identificazione**, **raccolta**, **acquisizione** e **preservazione**.
- Per prassi la copia forense si realizza come un **accertamento tecnico non ripetibile perché la maggior parte delle volte occorre accendere il dispositivo prima di realizzare l'acquisizione e questo può provocare la modifica di alcune informazioni contenute sulla memoria del dispositivo**



Criptofonini

- I criptofonini sono smartphone dotati di particolari sistemi di cifratura che li rendono potenzialmente inviolabili e a prova di intercettazione.
- Il sistema operativo installato disabilita la localizzazione GPS, i servizi Apple/Google, il Bluetooth, la fotocamera, la porta USB (che rimane in funzione solo per la carica della batteria), oscura le notifiche push e blocca ogni altro servizio che possa generare un rischio di intercettazione o localizzazione.
- Sia le telefonate sia le chat sono ovviamente crittografate, con cifratura a più livelli: crittografia Diffie-Hellman, a curve ellittiche (ECC), PGP (Pretty Good Privacy) per le email, OTR (Off-the-Record Messaging) per la chat e ZRTP per le chiamate (un protocollo per telefonate sicure che consente di effettuare chiamate criptate sulla rete Internet).
- La sicurezza e la segretezza di questi telefoni sono dunque fondate su almeno tre livelli:
  - Il dispositivo e il sistema operativo: vengono installati OS con sistemi antimanomissione e con livelli di protezione e di accesso multipli (autenticazione a due fattori, codici Captcha ecc.);
  - La connessione e le comunicazioni: il dispositivo si connette solo alla rete dedicata di server sicuri, non utilizza le reti pubbliche non sicure;
  - Le applicazioni: sono app dedicate, con crittografia forte. Sono inoltre dotate di funzionalità che limitano con password i tentativi di accesso ed hanno in genere funzioni di wiping che cancellano tutti i dati dell'app in caso di tentata violazione.

Criptofonini

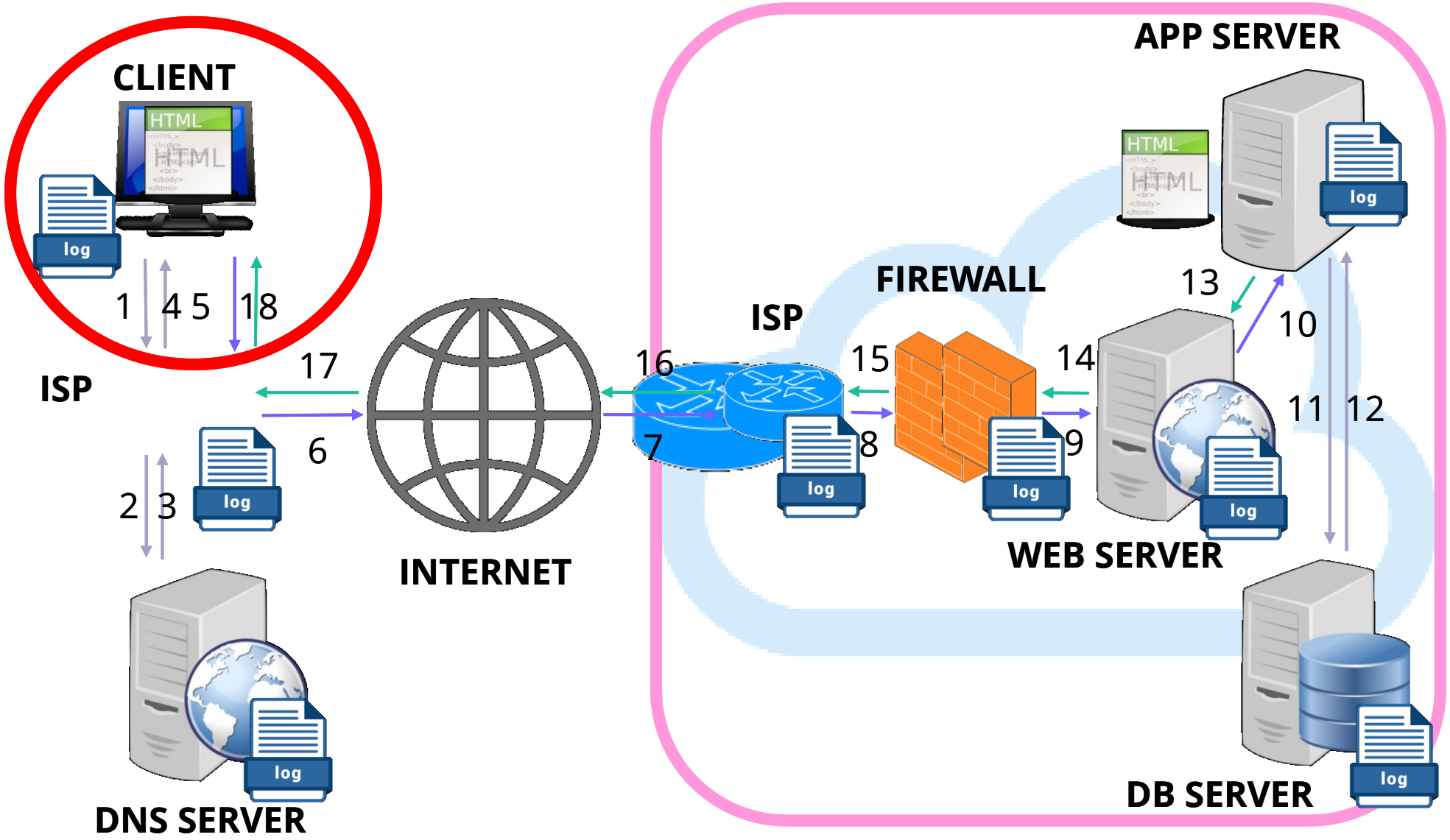


- Acquisire il criptofonino di un utente è un attività molto critica perché:
  - Sono impostate password molto complesse
  - Al loro interno sono presenti pochissime informazioni
  - Spesso sono attivi meccanismi di reset automatici
- Acquisire il server del provider con cui interagiscono gli utenti dei criptofonini è molto utile perchè:
  - Consente di ricostruire i contatti e i dispositivi utilizzati
  - Consente di ricavare le chiavi crittografiche utilizzate
  - Consente di conoscere la logica applicativa e gli algoritmi crittografici utilizzati
  - Consente di acquisire i logs e le comunicazioni in modalità originale e integrale

Acquisizione dalla piattaforma

- Poiché molte attività si svolgono online, attraverso l'uso di servizi internet (web, email, e-commerce, social network, e-banking, messaggistica, web call, ecc.) **è utile acquisire le informazioni direttamente dal provider attraverso la rete.**
- Esegue una copia forense di tutte le informazioni presenti in piattaforma.
- Ciò si rende necessario perché:
  - Il dispositivo che contiene le informazioni è distante o non facilmente raggiungibile
  - Le informazioni sono presenti solo sulla piattaforma
  - L'accesso alle memorie fisiche non è percorribile (rogatorie)
  - Non è facile individuare il luogo di memorizzazione (cloud)
  - È necessario acquisirle velocemente per criticità legate alla volatilità o alterabilità del dato
  - È un'ottima alternativa per acquisire informazioni non reperibile sui dispositivi fisici (backup smartphone, piattaforme di messaggistica, piattaforme di social network «facebook», «instagram», «tiktok», «likedin», «google», email, spazi virtuali «iCloud» «Google Drive» «DropBox» , ecc.

Web architecture



Metodologia

- Occorre procurarsi le credenziali di accesso
- Se richiesto, occorre modificare le credenziali di accesso per «sequestrare» il profilo
- Alcune piattaforme social offrono la possibilità di esportare tutti i dati associati ad un determinato profilo utente
- Si trovano molte più informazioni che sul dispositivo mobile
- Si procede acquisendo:
  - il contenuto visibile o scaricato,
  - il dato del traffico dati generato,
  - il video che cattura tutti i comandi e gli output generati (screen recorder)
  - infine, si applica una marca temporale

Promemoria

- Acquisire e analizzare l’intero percorso di comunicazione
- Incrociare le tracce temporali con i tabulati
- Ricordarsi che le evidenze digitali sono altamente volatili e facilmente alterabili
- Verificare l’integrità e la validità dei dati, anche con informazioni esterne
- Ricordarsi delle app di Intelligenza artificiale generativa

Contatti

www.vincenzocalabro.it

info@vincenzocalabro.it

LinkedIn vincenzocalabro