



**Ordine degli Ingegneri
della provincia di Napoli**

Seminario «Le intercettazioni telefoniche: Analisi tabulati e Geolocalizzazione»

NAPOLI - 08/03/2019

Ing. Giuseppe Caprio - Commissione ICT OIN



DI COSA VI PARLERO' ?

COSA E' E COME NASCE L'INFORMATICA FORENSE

-

L'INQUADRAMENTO NORMATIVO

-

ESEMPI REVERSE ENGINEERING

DEFINIZIONE

La Computer Forensics (Informatica Forense) è la scienza che studia :

- ***l'individuazione,***
- ***la conservazione,***
- ***la protezione,***
- ***l'estrazione,***
- ***la documentazione***

e ogni altra forma di trattamento del dato informatico per essere valutato in un processo giuridico e studia, ai fini probatori, le tecniche e gli strumenti per l'esame metodologico dei sistemi informatici

OBBIETTIVI

individuazione di informazioni aventi valore probatorio (*evidenze digitali*)

Si basa sull'interpretazione e correlazione dei dati memorizzati su un sistema digitale (*artefatti*) al fine di ricostruire le azioni effettuate mediante quel sistema

Come nasce - Convenzione di Budapest

- La Convenzione del 23 novembre 2001 è il primo trattato internazionale sulle infrazioni penali commesse via internet e su altre reti informatiche, e tratta in particolare le violazioni dei diritti d'autore, la frode informatica, la pornografia infantile e le violazioni della sicurezza della rete. **Contiene inoltre una serie di misure e procedure appropriate, quali la perquisizione dei sistemi di reti informatiche e l'intercettazione dei dati.**
- Il suo **obiettivo** principale, enunciato nel preambolo, è **perseguire una politica penale comune per la protezione della società contro la cybercriminalità, in special modo adottando legislazioni appropriate e promuovendo la cooperazione internazionale.**

Norma Italiana - Legge 48/2008

247

- **C.P.P. “Casi e forme delle perquisizioni”** - > adottare misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione

254-
bis

- **Sequestro di dati informatici presso fornitori di servizi informatici, telematici e di telecomunicazioni** -> l'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

259

- **Custodia delle cose sequestrate** -> Quando la custodia riguarda dati, informazioni o programmi informatici, il custode è altresì avvertito dell'obbligo di **impedirne l'alterazione o l'accesso da parte di terzi**, salva, in quest'ultimo caso, diversa disposizione dell'autorità giudiziaria

260

- **Apposizione dei sigilli alle cose sequestrate. Cose deperibili** -> «Quando si tratta di dati, di informazioni o di programmi informatici, la copia deve essere realizzata su adeguati supporti, mediante **procedura che assicuri la conformità della copia all'originale e la sua immodificabilità**; in tali casi, la custodia degli originali può essere disposta anche in luoghi diversi dalla cancelleria o dalla segreteria»

352

- **Perquisizioni** -> **gli ufficiali di polizia giudiziaria, adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione**

354

- **Accertamenti urgenti sui luoghi, sulle cose e sulle persone. Sequestro** -> gli ufficiali della polizia giudiziaria adottano, altresì, le misure tecniche o impartiscono le prescrizioni necessarie ad **assicurarne la conservazione e ad impedirne l'alterazione** e l'accesso e provvedono, ove possibile, alla loro immediata duplicazione su adeguati supporti, mediante una procedura che assicuri la conformità della copia all'originale e la sua immodificabilità.



Legge 48/2008

- Impedire l'alterazione
- Conformità delle copie
- Impedire l'accesso di terzi
- Conservazione

QUANDO SERVE UNA CONSULENZA TECNICA?

**in qualunque caso in cui si ha bisogno
che il dato informatico diventi una**

EVIDENZA DIGITALE

**FURTO, FRODE, RICATTO, STALKING, CYBER BULLISMO,
DIVORZIO, LICENZIAMENTO DIPENDENTE INFEDELE,
VIOLAZIONE RETI AZIENDALI, SPIONAGGIO,
PEDOPORNOGRAFIA, DECESSO, TERRORISMO**



QUANDO SI DA SUPPORTO A : GIUDICE CIVILE

CTU- CONSULENTE TECNICO DI UFFICIO

art. 191 Codice di Procedura Civile

il giudice istruttore, con ordinanza ai sensi dell'articolo 183, settimo comma, o con altra successiva ordinanza (2), **nomina un consulente, formula i quesiti e fissa l'udienza nella quale il consulente deve comparire**

QUANDO SI DA SUPPORTO A : GIUDICE PENALE

PERITO – conferimento incarico art. 226 Codice di Procedura Penale

1. Il giudice, accertate le generalità del perito, gli chiede se si trova in una delle condizioni previste dagli articoli 222 e 223, lo avverte degli obblighi e delle responsabilità previste dalla legge penale e lo invita a rendere la seguente dichiarazione: «consapevole della responsabilità morale e giuridica che assumo nello svolgimento dell'incarico, mi impegno ad adempiere al mio ufficio senza altro scopo che quello di far conoscere la verità e a mantenere il segreto su tutte le operazione peritali» .
2. Il giudice formula quindi i quesiti, sentiti il perito, i consulenti tecnici [225], il pubblico ministero e i difensori presenti.

QUANDO SI DA SUPPORTO A : GIUDICE PENALE

PERITO – Art. 222 incapacità e incompatibilità

1. Non può prestare ufficio di perito, a pena di nullità [144, 177-186]:
 - a) il minorenne, l'interdetto, l'inabilitato e chi è affetto da infermità di mente;
 - b) chi è interdetto anche temporaneamente dai pubblici uffici [289; att. 69 3; c.p. 28] ovvero è interdetto o sospeso dall'esercizio di una professione o di un'arte [290; att. 69 3; c.p. 30 e 35];
 - c) chi è sottoposto a misure di sicurezza personali [c.p. 215] o a misure di prevenzione;
 - d) chi non può essere assunto come testimone o ha facoltà di astenersi dal testimoniare o chi è chiamato a prestare ufficio di testimone [194] o di interprete [143];
 - e) chi è stato nominato consulente tecnico [225, 233, 360] nello stesso procedimento o in un procedimento connesso [12]

QUANDO SI DA SUPPORTO A : GIUDICE PENALE

PERITO – Art. 223 C.P.P. - ASTENSIONE

1. Quando esiste un motivo di astensione, il perito ha l'obbligo di dichiararlo.
2. Il perito può essere ricusato dalle parti nei casi previsti dall'articolo 36 a eccezione di quello previsto dal comma 1 lettera h) del medesimo articolo.
3. La dichiarazione di astensione o di ricusazione [145] può essere presentata fino a che non siano esaurite le formalità di conferimento dell'incarico [226] e, quando si tratti di motivi sopravvenuti ovvero conosciuti successivamente, prima che il perito abbia dato il proprio parere
4. Sulla dichiarazione di astensione o di ricusazione decide, con ordinanza, il giudice che ha disposto la perizia.
5. Si osservano, in quanto applicabili, le norme sulla ricusazione del giudice [37].

QUANDO SI DA SUPPORTO A : GIUDICE PENALE

PERITO – Art. 36 C.P.P. - ASTENSIONE

- a) se ha interesse nel procedimento o se alcuna delle parti private o un difensore è debitore o creditore di lui, del coniuge o dei figli;
- b) se è tutore, curatore, procuratore o datore di lavoro di una delle parti private ovvero se il difensore, procuratore o curatore di una di dette parti è prossimo congiunto [307 c.p.] di lui o del coniuge;
- c) se ha dato consigli o manifestato il suo parere sull'oggetto del procedimento fuori dell'esercizio delle funzioni giudiziarie;
- d) se vi è inimicizia grave fra lui o un suo prossimo congiunto e una delle parti private;
- e) se alcuno dei prossimi congiunti di lui o del coniuge è offeso [90 c.p.p.] o danneggiato dal reato o parte privata;
- h) se esistono altre gravi ragioni di convenienza (3).

QUANDO SI DA SUPPORTO AL : PUBBLICO MINISTERO/PRIVATI

CT- CONSULENTE TECNICO

Art. 225 C.P.P. - NOMINA DEL CONSULENTE TECNICO

1. Disposta la perizia, il pubblico ministero e le parti private hanno facoltà di nominare propri consulenti tecnici in numero non superiore, per ciascuna parte, a quello dei periti.
2. Le parti private, nei casi e alle condizioni previste dalla legge sul patrocinio statale dei non abbienti, hanno diritto di farsi assistere da un consulente tecnico a spese dello Stato [98].
3. Non può essere nominato consulente tecnico chi si trova nelle condizioni indicate nell'articolo 222 comma 1 lettere a), b), c), d).

Art. 233 C.P.P. - CT fuori dai casi di Perizia

QUANDO SI DA SUPPORTO AL : PUBBLICO MINISTERO

CT- CONSULENTE TECNICO

Art. 359 C.P.P. - CONSULENTI TECNICI DEL PM

1. Il pubblico ministero, quando procede ad accertamenti, rilievi segnaletici, descrittivi o fotografici e ad ogni altra operazione tecnica per cui sono necessarie specifiche competenze, può nominare e avvalersi di consulenti, che non possono rifiutare la loro opera [233].
2. Il consulente può essere autorizzato dal pubblico ministero ad assistere a singoli atti di indagine.

QUANDO SI DA SUPPORTO AL : PUBBLICO MINISTERO

CT- CONSULENTE TECNICO

Art. 360 C.P.P. - Accertamenti tecnici NON RIPETIBILI

1. Quando gli accertamenti previsti dall'articolo 359 riguardano persone, cose o luoghi il cui stato è soggetto a modificazione, il pubblico ministero avvisa, senza ritardo, la persona sottoposta alle indagini [61], la persona offesa [90] dal reato e i difensori del giorno, dell'ora e del luogo fissati per il conferimento dell'incarico e della facoltà di nominare consulenti tecnici [225, 233].
2. Si applicano le disposizioni dell'articolo 364 comma 2.
3. I difensori nonché i consulenti tecnici eventualmente nominati hanno diritto di assistere al conferimento dell'incarico, di partecipare agli accertamenti e di formulare osservazioni e riserve .

OMISSIS

PERCHE' IL DATO DIGITALE DIVENTA EVIDENZA DIGITALE ATTRAVERSO PROCESSI DEFINITI

ISO 27037/2012

“Guidelines for identification, collection, acquisition and preservation of digital evidence”



Si occupa del Trattamento del reperto informatico e dell'integrità della prova informatica e metodologia al fine di rendere ammissibile la prova in giudizio



si limita alle fasi iniziali del processo di gestione della prova informatica, non arriva all'analisi, non si occupa di aspetti legali, strumenti, reportistica, trattamento dei dati

Perché SERVONO COMPETENZE degli operatori, in modo che si evitino errori e il dato digitale possa assumere valore probatorio, e quindi essere una evidenza digitale, che soddisfa le proprietà:

- ❑ **Integrità:** *assenza di alterazioni negli artefatti*
- ❑ **Completezza:** *analisi di tutti gli artefatti ad essa riferibili*
- ❑ **Autenticità:** *certezza della provenienza degli artefatti*
- ❑ **Veridicità:** *correttezza dell'interpretazione degli artefatti e delle azioni che ne hanno determinato la comparsa*

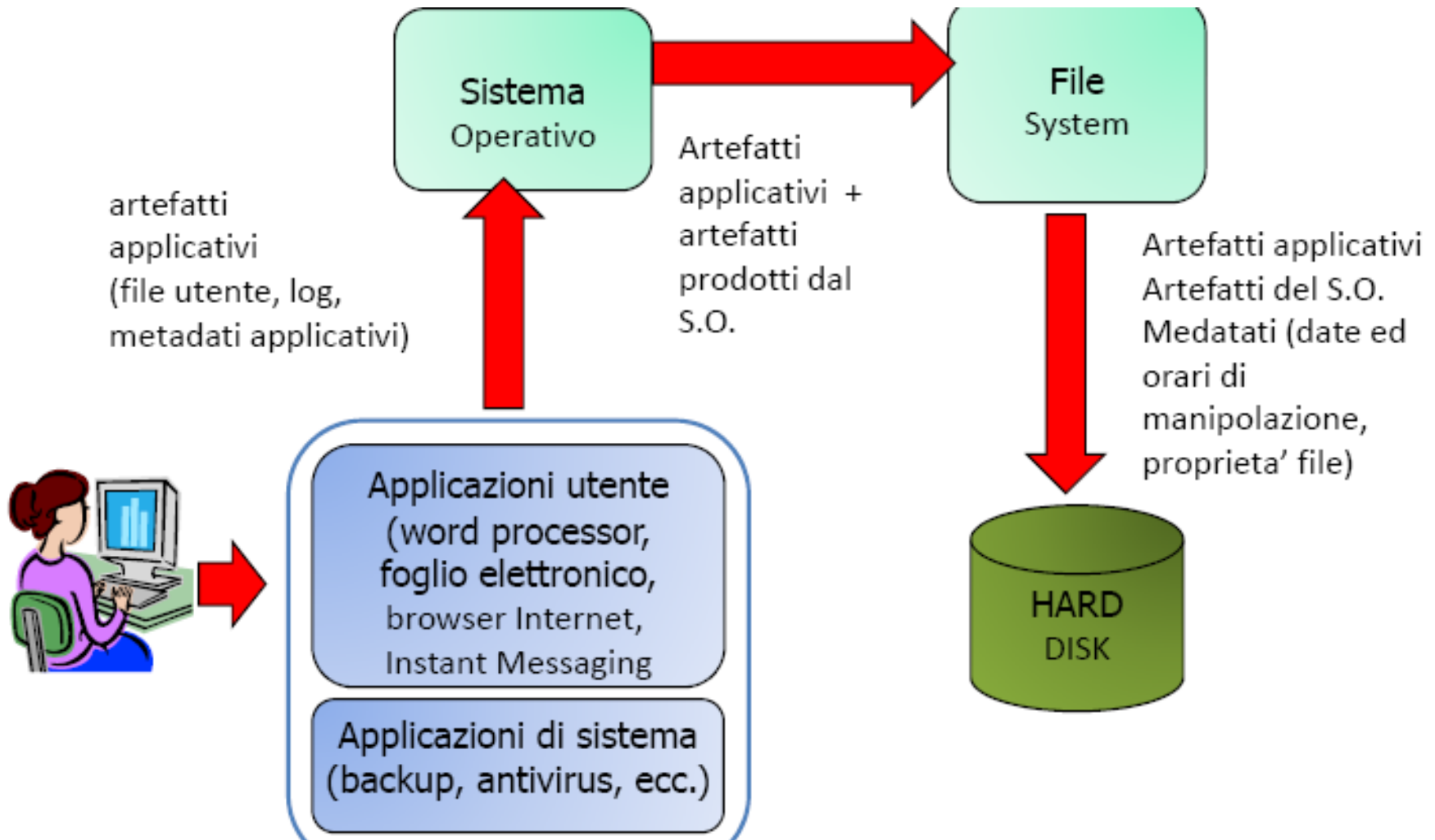


**SERVE L'INGEGNERE
perché l'acquisizione e l'analisi dei
sistemi non si riduce all'uso di semplici
macchinari o software**

A VOLTE (SEMPRE PIU' SPESSO)

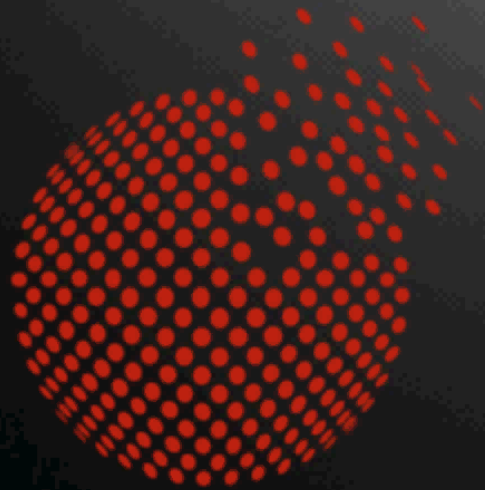
**SI DEVONO INTERPRETARE E
ANALIZZARE I DATI ESTRATTI**

ESEMPIO ALIBI INFORMATICO





ESEMPIO ALIBI INFORMATICO



FUTURE
engineering

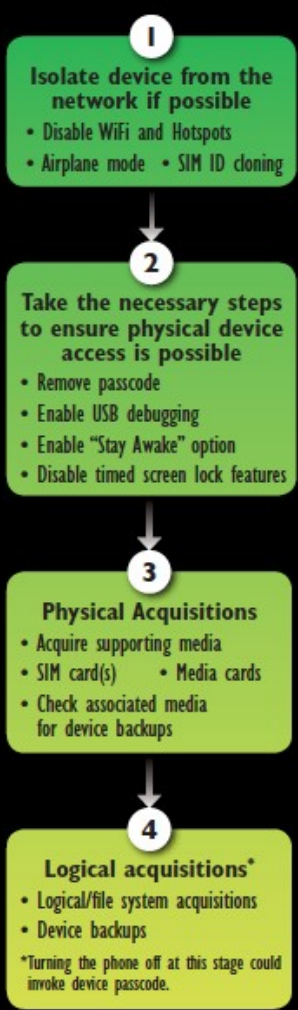


SERVE L'INGEGNERE
perché l'acquisizione e l'analisi dei
sistemi non si riduce all'uso di "semplici"
macchinari o software

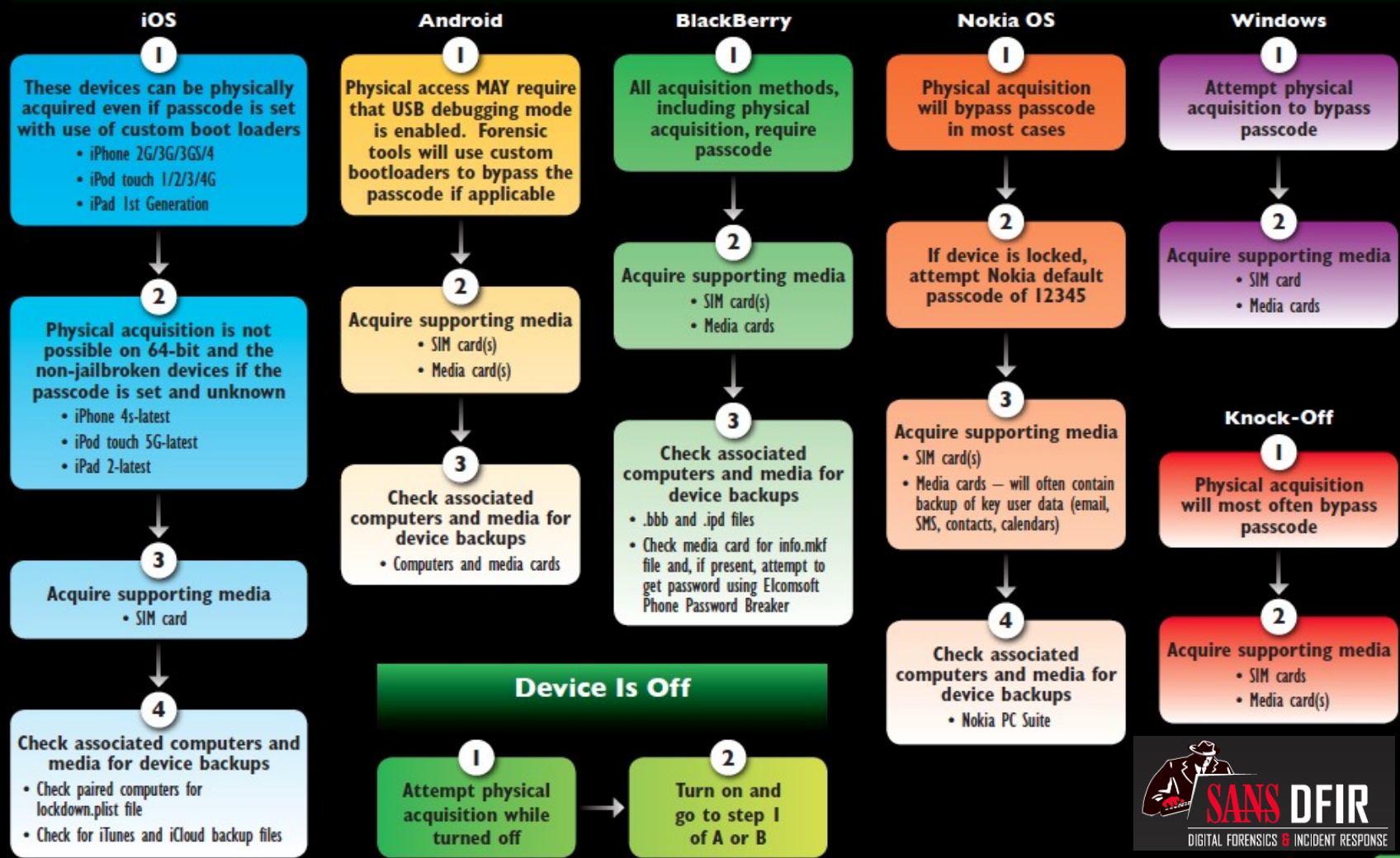
A VOLTE (SEMPRE PIU' SPESSO)
SI DEVONO TROVARE SOLUZIONI
A PROBLEMI COMPLESSI

Smartphone Acquisition Guide

A Device On & Unlocked



B Device On & Locked



ESEMPIO SISTEMA ANDROID PRODUTTORE – HUAWEI

- dispositivo non supportato da macchinari per l'acquisizione fisica con dispositivo spento
- all'accensione risulta bloccato con Pattern

Android

1

Physical access **MAY** require that USB debugging mode is enabled. Forensic tools will use custom bootloaders to bypass the passcode if applicable

2

Acquire supporting media

- SIM card(s)
- Media card(s)

3

Check associated computers and media for device backups

- Computers and media cards

Quindi da prassi non posso fare niente altro, oppure si ???

ESEMPIO ANDROID

VERIFICO SE E' STATO ESEGUITO IL ROOTING DEL
DISPOSITIVO E SE RISULTA INSTALLATA UNA
APPLICAZIONE DI CUSTOM RECOVERY

QUINDI AVVIO IN DISPOSITIVO
NELLA MODALITA' RECOVERY

E.....INCROCIO LE DITA

ESEMPIO ANDROID

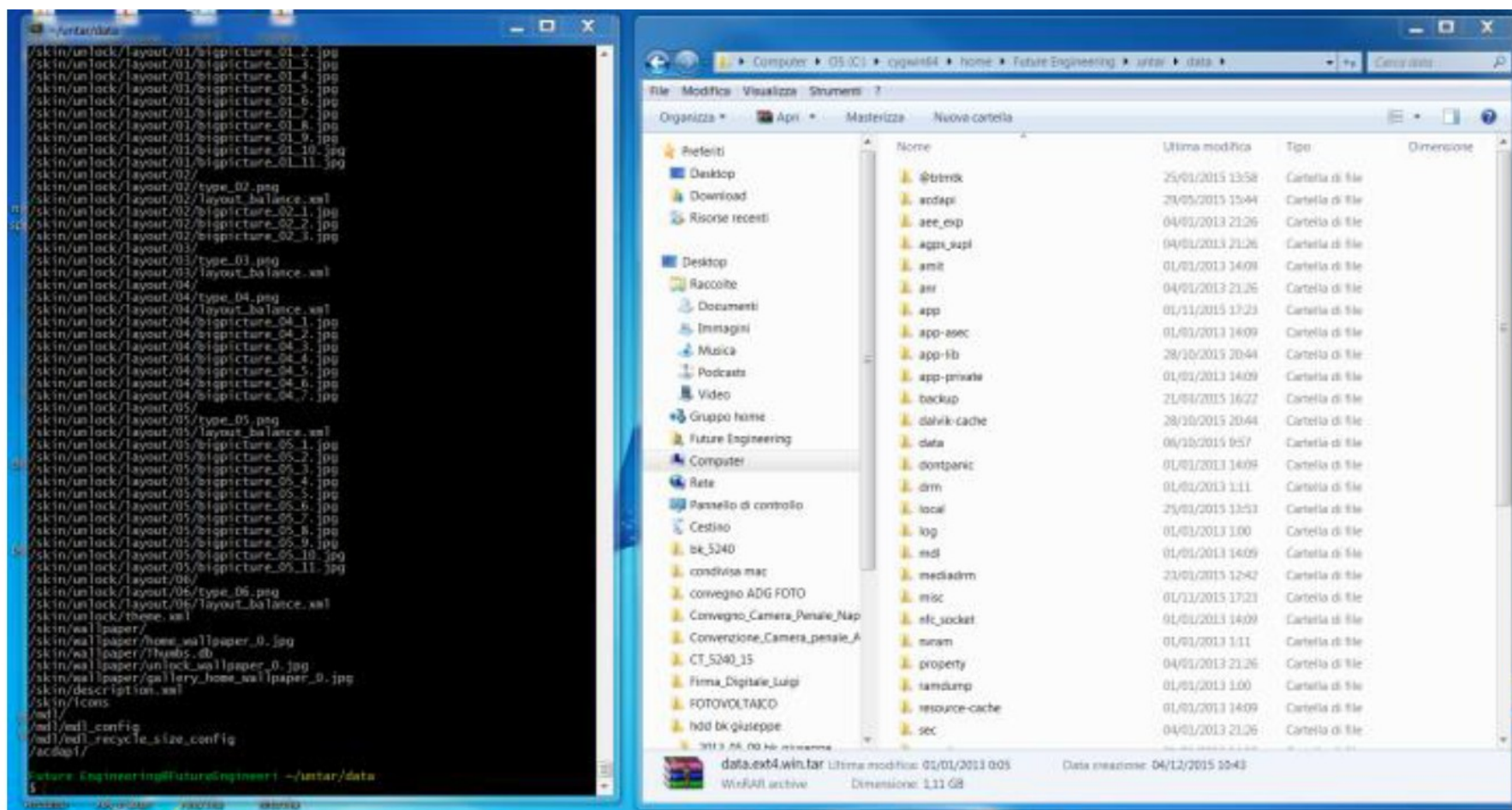
SONO FORTUNATO,
RISULTA INSTALATA
TWRP

POSSO ESEGUIRE
UN BACKUP
COMPLETO

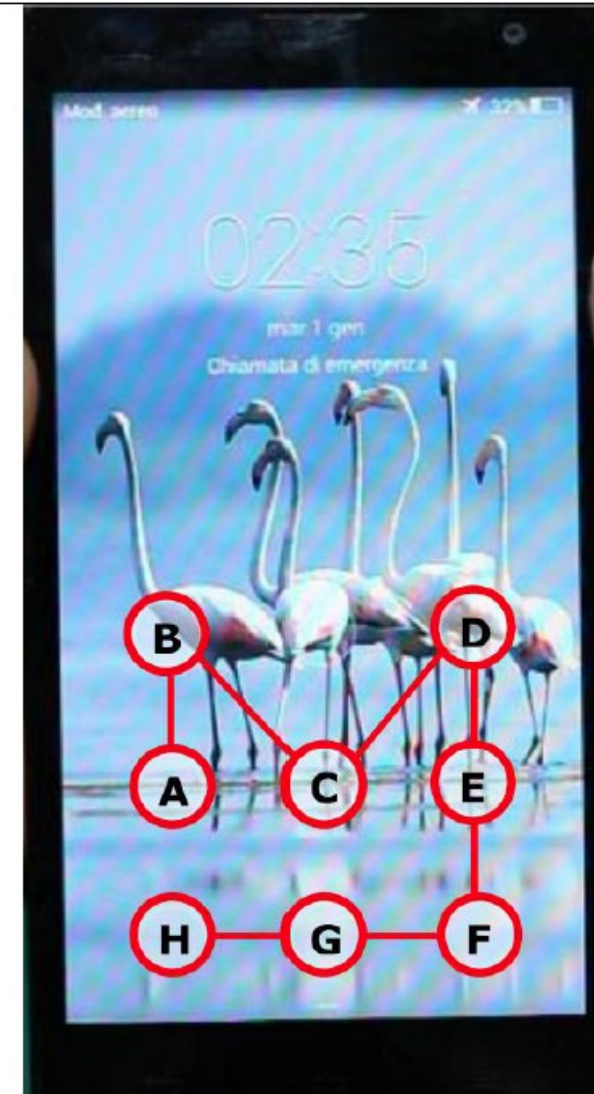
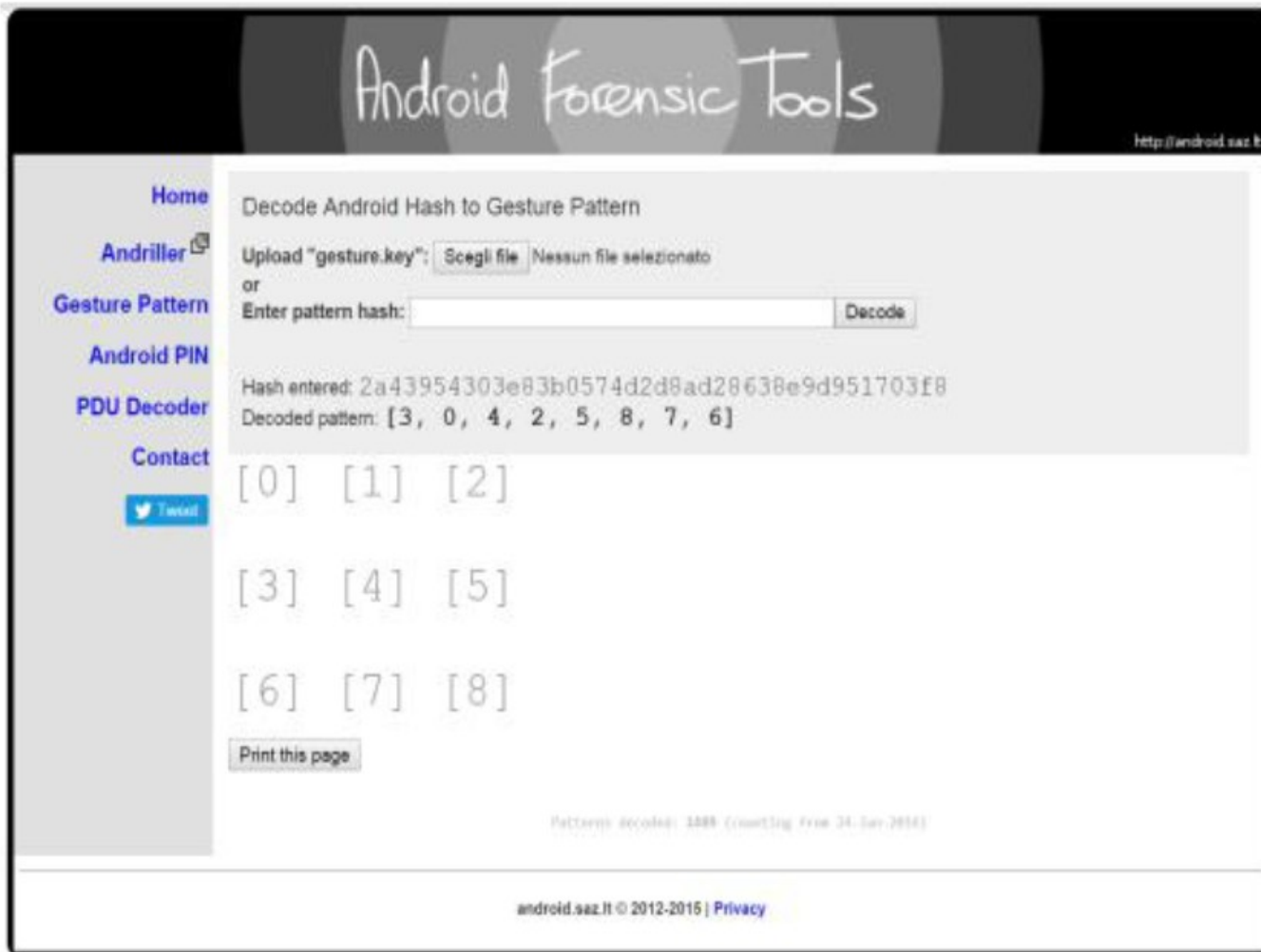


ESEMPIO ANDROID

SALVATO IL BACKUP SUL PC POSSO DECODIFICARLO
E RECUPERARE LA “gesture.key”



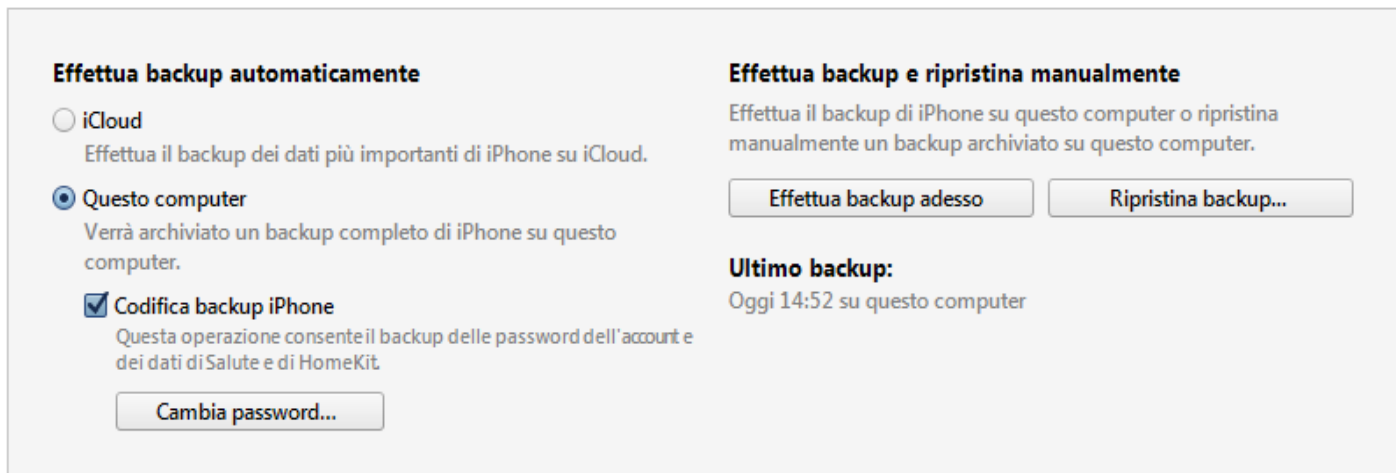
ESEMPIO ANDROID



ESEMPIO iPhone e MacBook

1- iPhone sbloccato, ma backup criptato

Backup



The screenshot shows the 'Backup' settings on an iPhone. It is divided into two main sections: 'Effettua backup automaticamente' and 'Effettua backup e ripristina manualmente'. In the first section, 'Questo computer' is selected, and 'Codifica backup iPhone' is checked. In the second section, there are buttons for 'Effettua backup adesso' and 'Ripristina backup...', and the 'Ultimo backup' is noted as 'Oggi 14:52 su questo computer'.

Effettua backup automaticamente

- iCloud
Effettua il backup dei dati più importanti di iPhone su iCloud.
- Questo computer
Verrà archiviato un backup completo di iPhone su questo computer.
- Codifica backup iPhone
Questa operazione consente il backup delle password dell'account e dei dati di Salute e di HomeKit.
[Cambia password...](#)

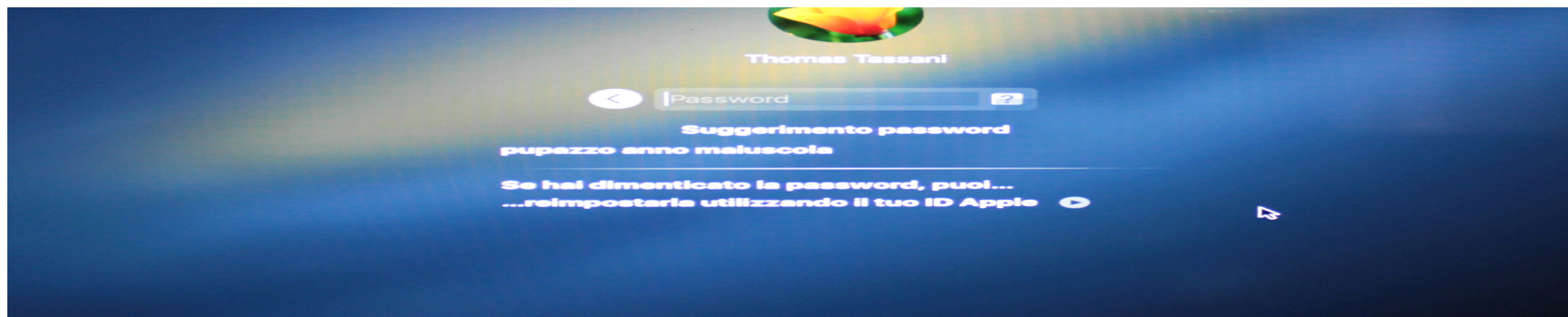
Effettua backup e ripristina manualmente

Effettua il backup di iPhone su questo computer o ripristina manualmente un backup archiviato su questo computer.

[Effettua backup adesso](#) [Ripristina backup...](#)

Ultimo backup:
Oggi 14:52 su questo computer

2- MacBook con password di accesso



ESEMPIO iPhone e MacBook

1- iPhone
sbloccato, ma
backup criptato



2- MacBook con
password di
accesso



ESEMPIO iPhone e MacBook

NON BASTA
PREMERE IL
BOTTONE

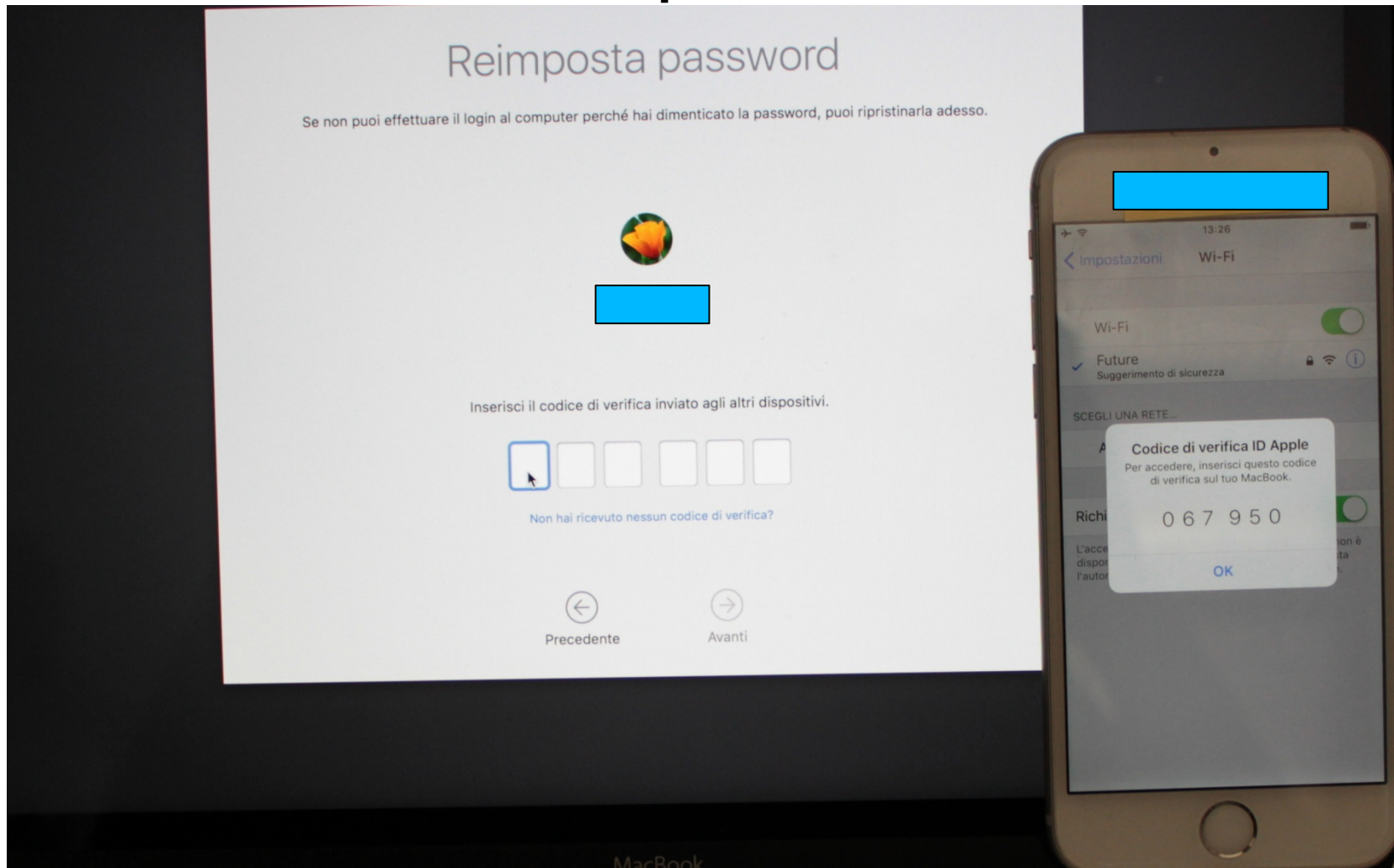


NON RIESCO AD
AVERE DATI
UTILIZZABILI



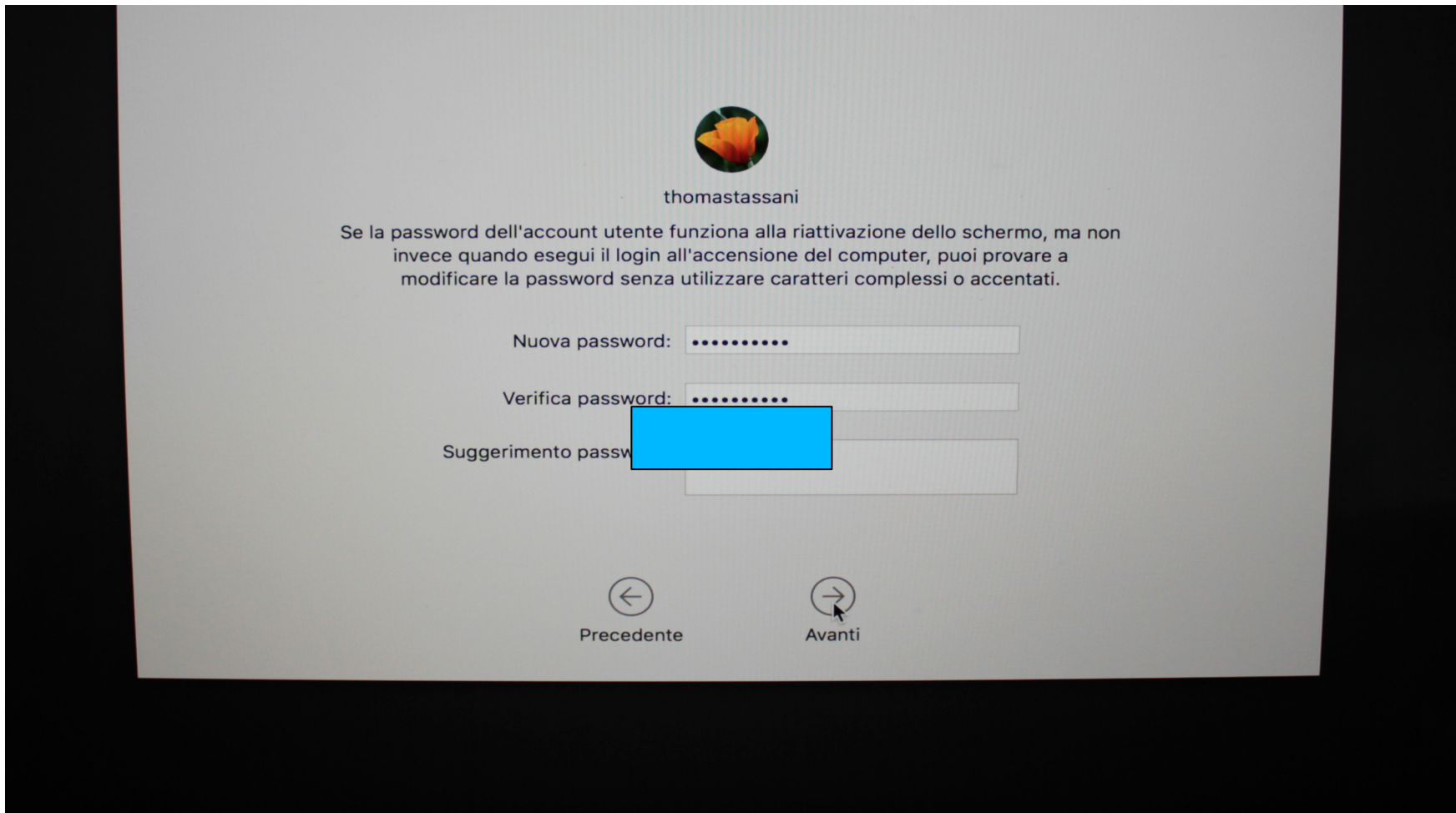
ESEMPIO iPhone e MacBook

2- MacBook con password di accesso



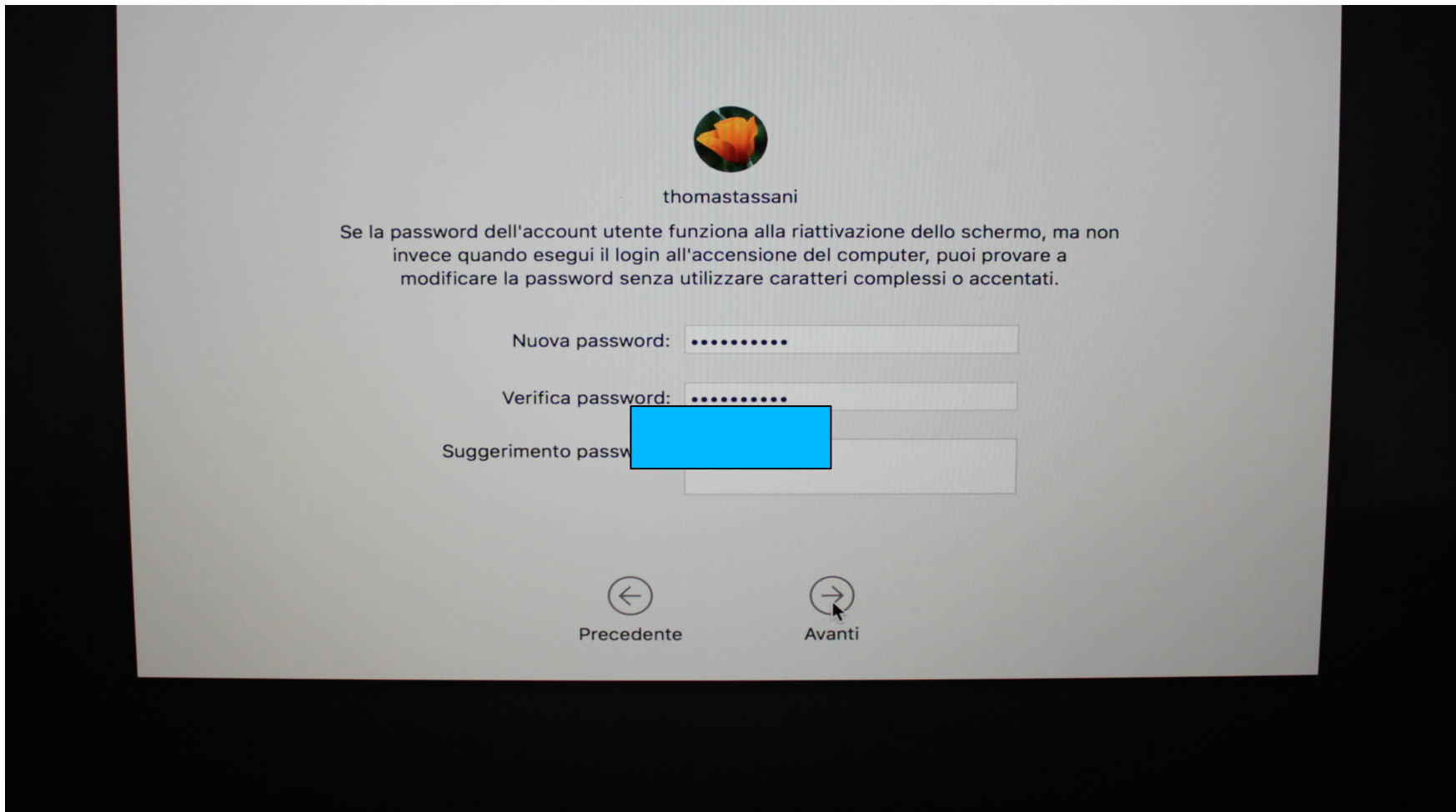
ESEMPIO iPhone e MacBook

2- MacBook -> cambio password di accesso



ESEMPIO iPhone e MacBook

2- MacBook -> cambio password di accesso



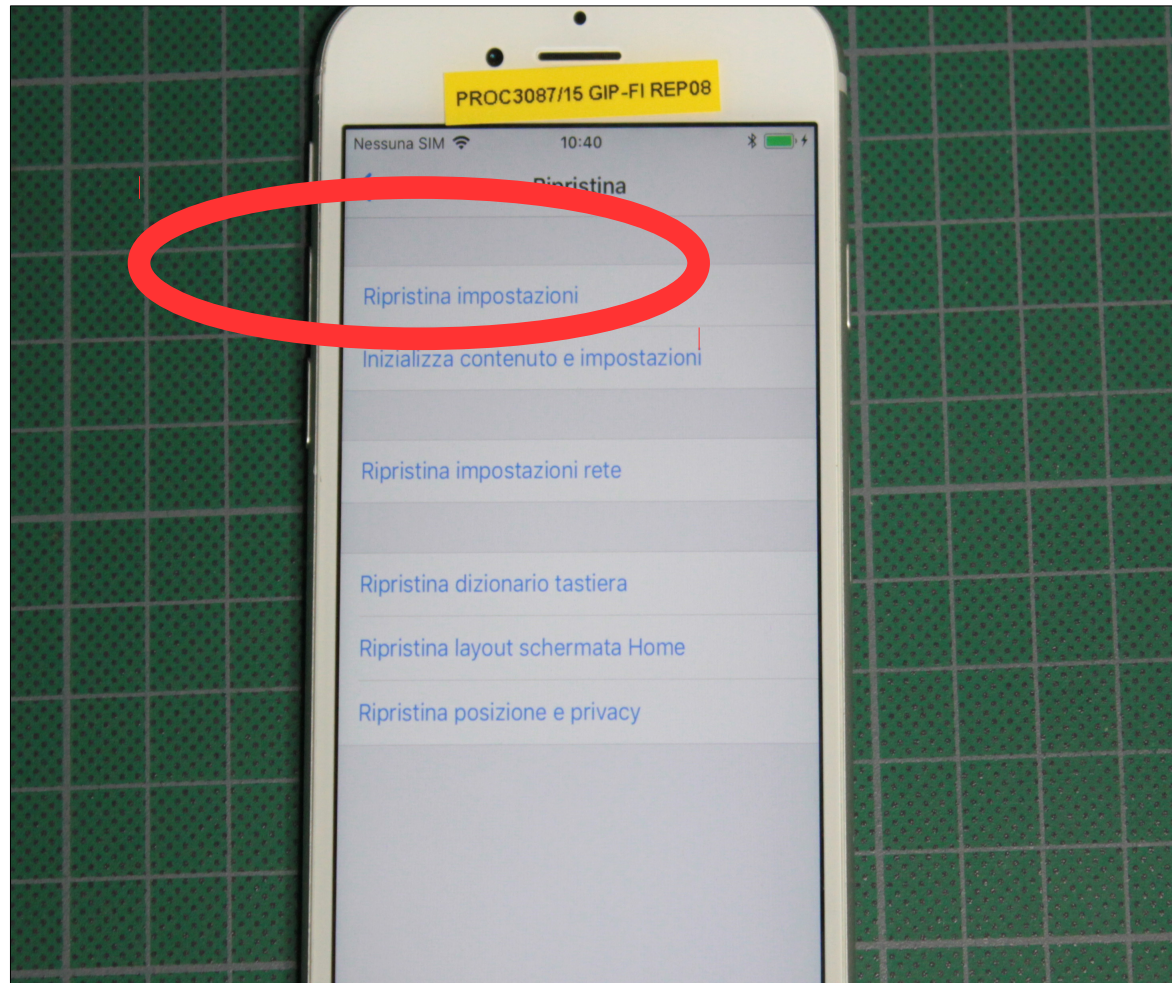
ESEMPIO iPhone e MacBook

1- iPhone sbloccato -> backup senza password

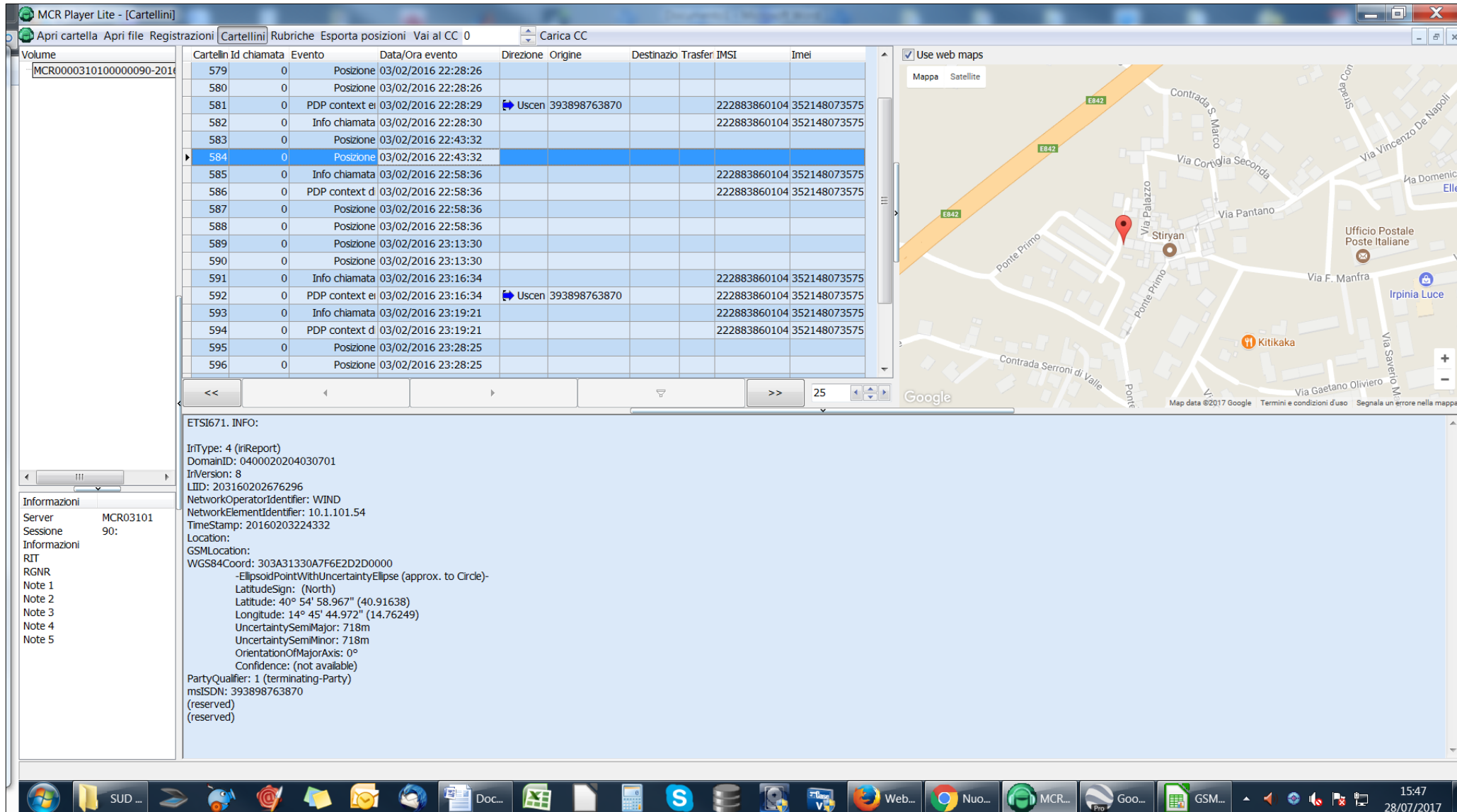
Impostazioni

→ Generali

→ Ripristina



ESEMPIO - geolocalizzazione con sistemi di intercettazione



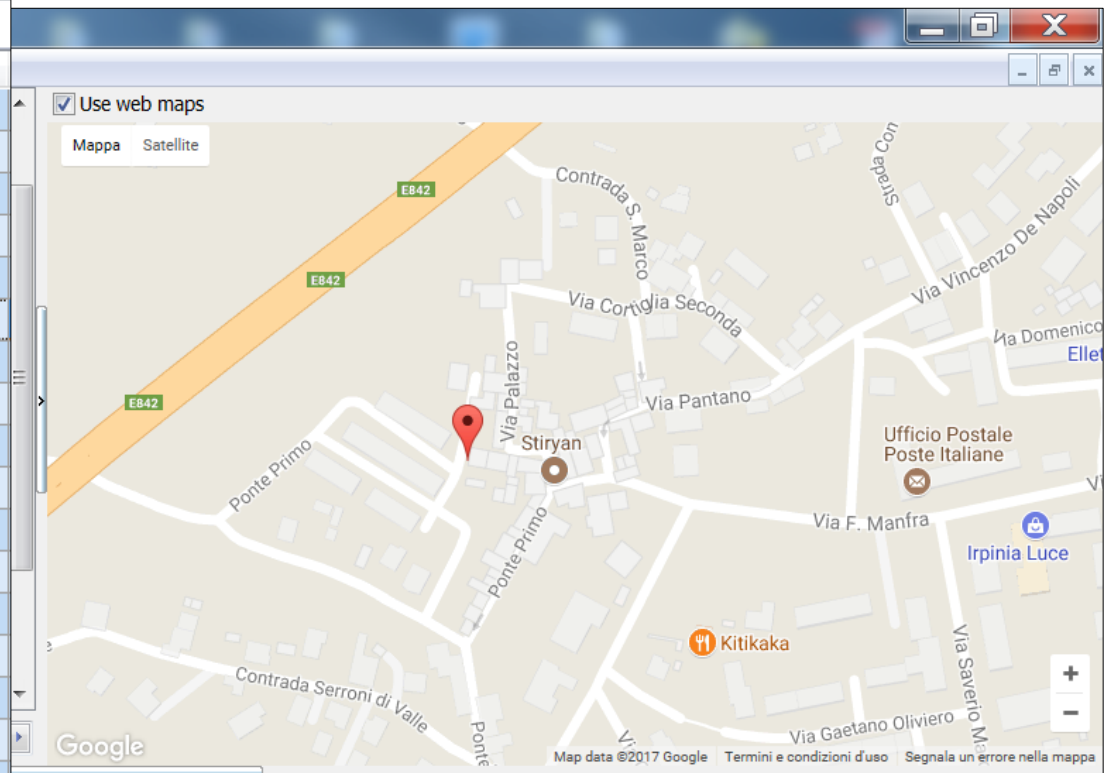
The screenshot displays the MCR Player Lite interface. On the left, a table lists call events with columns for Call ID, Event, Date/Time, Direction, Origin, Destination, IMSI, and IMEI. Row 584 is highlighted. On the right, a Google Map shows a location pin in the area of Ponte Primo, with a red location marker and a red location pin. Below the map, technical details for ETSI671 are shown, including IrType, DomainID, IrVersion, LIID, NetworkOperatorIdentifier, NetworkElementIdentifier, TimeStamp, Location, GSMLocation, WGS84Coord, and PartyQualifier.

Cartellini	Id chiamata	Evento	Data/Ora evento	Direzione	Origine	Destinazio	Trasfer	IMSI	Imei
	579	0	Posizione	03/02/2016 22:28:26					
	580	0	Posizione	03/02/2016 22:28:26					
	581	0	PDP context ei	03/02/2016 22:28:29	Usccn	393898763870		222883860104	352148073575
	582	0	Info chiamata	03/02/2016 22:28:30				222883860104	352148073575
	583	0	Posizione	03/02/2016 22:43:32					
	584	0	Posizione	03/02/2016 22:43:32					
	585	0	Info chiamata	03/02/2016 22:58:36				222883860104	352148073575
	586	0	PDP context d	03/02/2016 22:58:36				222883860104	352148073575
	587	0	Posizione	03/02/2016 22:58:36					
	588	0	Posizione	03/02/2016 22:58:36					
	589	0	Posizione	03/02/2016 23:13:30					
	590	0	Posizione	03/02/2016 23:13:30					
	591	0	Info chiamata	03/02/2016 23:16:34				222883860104	352148073575
	592	0	PDP context ei	03/02/2016 23:16:34	Usccn	393898763870		222883860104	352148073575
	593	0	Info chiamata	03/02/2016 23:19:21				222883860104	352148073575
	594	0	PDP context d	03/02/2016 23:19:21				222883860104	352148073575
	595	0	Posizione	03/02/2016 23:28:25					
	596	0	Posizione	03/02/2016 23:28:25					

ETSIG671. INFO:
 IrType: 4 (IrReport)
 DomainID: 0400020204030701
 IrVersion: 8
 LIID: 203160202676296
 NetworkOperatorIdentifier: WIND
 NetworkElementIdentifier: 10.1.101.54
 TimeStamp: 20160203224332
 Location:
 GSMLocation:
 WGS84Coord: 303A31330A7F6E2D2D0000
 -EllipsoidPointWithUncertaintyEllipse (approx. to Circle)-
 LatitudeSign: (North)
 Latitude: 40° 54' 58.967" (40.91638)
 Longitude: 14° 45' 44.972" (14.76249)
 UncertaintySemiMajor: 718m
 UncertaintySemiMinor: 718m
 OrientationOfMajorAxis: 0°
 Confidence: (not available)
 PartyQualifier: 1 (terminating-Party)
 msISDN: 393898763870
 (reserved)
 (reserved)

ESEMPIO - geolocalizzazione con sistemi di intercettazione

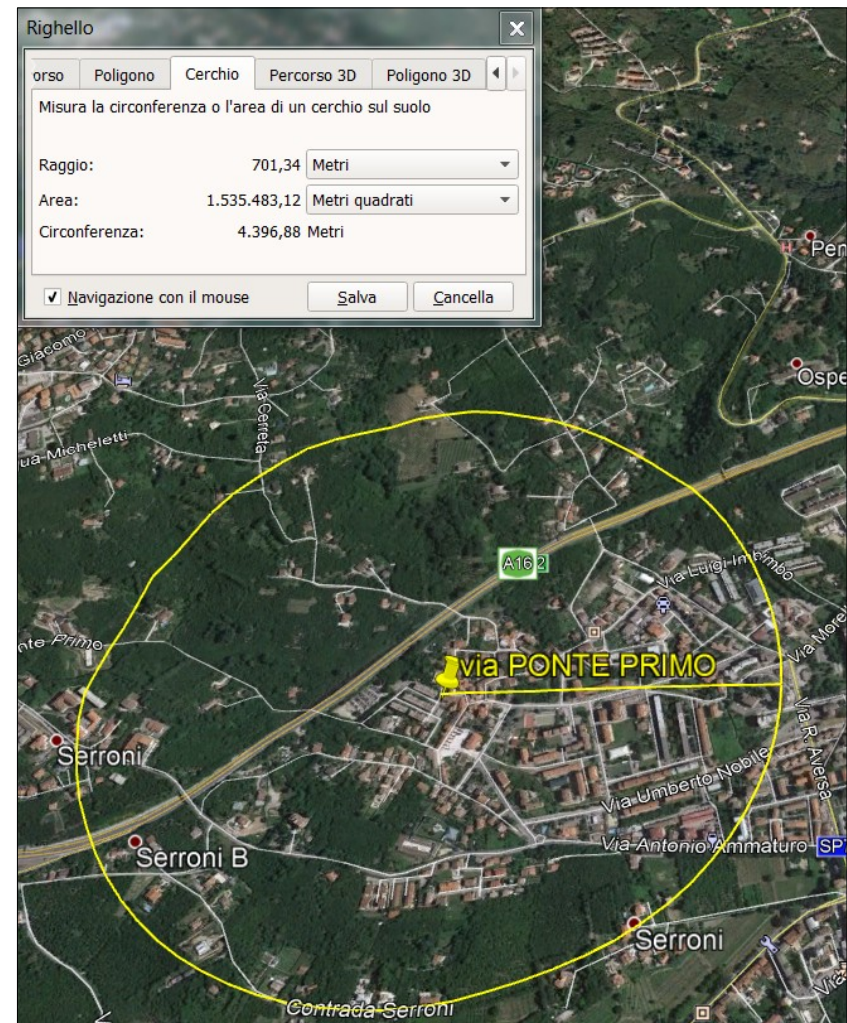
Cartellin	Id chiamata	Evento	Data/Ora evento
579	0	Posizione	03/02/2016 22:28:26
580	0	Posizione	03/02/2016 22:28:26
581	0	PDP context ei	03/02/2016 22:28:29
582	0	Info chiamata	03/02/2016 22:28:30
583	0	Posizione	03/02/2016 22:43:32
584	0	Posizione	03/02/2016 22:43:32
585	0	Info chiamata	03/02/2016 22:58:36
586	0	PDP context d	03/02/2016 22:58:36
587	0	Posizione	03/02/2016 22:58:36
588	0	Posizione	03/02/2016 22:58:36
589	0	Posizione	03/02/2016 23:13:30
590	0	Posizione	03/02/2016 23:13:30
591	0	Info chiamata	03/02/2016 23:16:34
592	0	PDP context ei	03/02/2016 23:16:34
593	0	Info chiamata	03/02/2016 23:19:21
594	0	PDP context d	03/02/2016 23:19:21
595	0	Posizione	03/02/2016 23:28:25
596	0	Posizione	03/02/2016 23:28:25

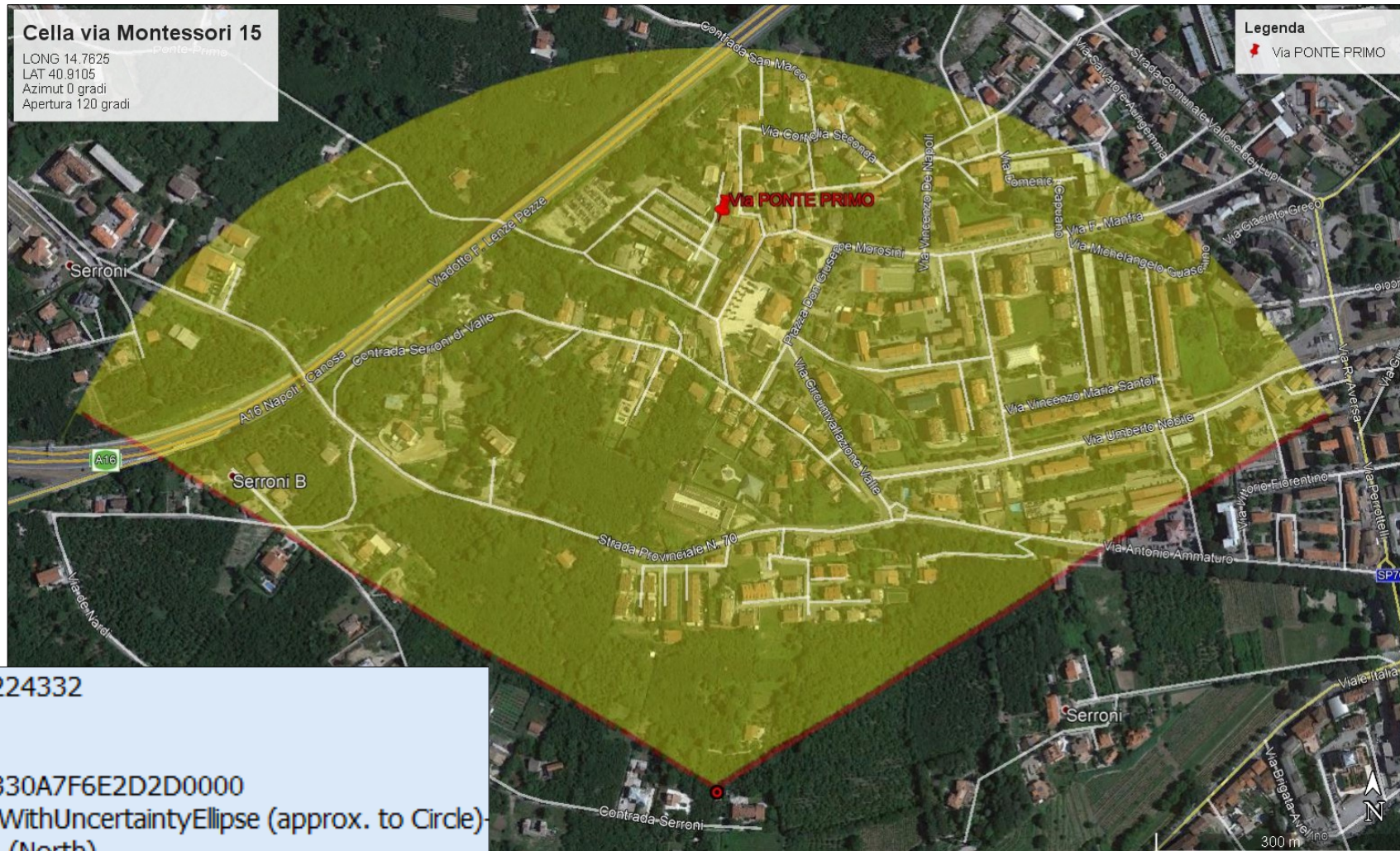


ESEMPIO - geolocalizzazione con sistemi di intercettazione

ETSI671. INFO:

IriType: 4 (iriReport)
 DomainID: 0400020204030701
 IriVersion: 8
 LIID: 203160202676296
 NetworkOperatorIdentifier: WIND
 NetworkElementIdentifier: 10.1.101.54
 TimeStamp: 20160203224332
 Location:
 GSMLocation:
 WGS84Coord: 303A31330A7F6E2D2D0000
 -EllipsoidPointWithUncertaintyEllipse (approx. to Circle)-
 LatitudeSign: (North)
 Latitude: 40° 54' 58.967" (40.91638)
 Longitude: 14° 45' 44.972" (14.76249)
 UncertaintySemiMajor: 718m
 UncertaintySemiMinor: 718m
 OrientationOfMajorAxis: 0°
 Confidence: (not available)
 PartyQualifier: 1 (terminating-Party)





Cella via Montessori 15

LONG 14.7625
LAT 40.9105
Azimut 0 gradi
Apertura 120 gradi

TimeStamp: 20160203224332

Location:

GSMLocation:

WGS84Coord: 303A31330A7F6E2D2D0000

-EllipsoidPointWithUncertaintyEllipse (approx. to Circle)

LatitudeSign: (North)

Latitude: 40° 54' 58.967" (40.91638)

Longitude: 14° 45' 44.972" (14.76249)

UncertaintySemiMajor: 718m

UncertaintySemiMinor: 718m

OrientationOfMajorAxis: 0°

Confidence: (not available)



Ordine degli Ingegneri
della provincia di Napoli

GRAZIE PER L'ATTENZIONE

Ing. Giuseppe Caprio
Commissione ICT OIN