DFA 10 aprile 2019

La Computer Forensics vista dal vivo

FORENSICA

Barbara Indovina

Tribunale di Roma (1)

- Il padre di G., 13 anni, denuncia due soggetti (A. e B.) che mediante chat whatsapp hanno instaurato iniziato a chattare con la figlia conosciuta in rete;
- Alla denuncia allega la stampa delle due chat;
- G. riferisce di avere 15 anni e non 13;
- A. non invia immagini erotiche alla ragazza, dialoga con lei per quasi un mese chiedendole di lei e raccontando della sua vita privata. Le dice che è «una bella cucciolotta» e «molto carina», lui abita a nord e lei a sud, le chiede solo se è mai stata nella sua città ma non la invita mai e non le chiede mai di vedersi.
- B. dialoga meno con la ragazza ma è molto insistente circa il fatto di vedersi, le richiede foto nuda e un giorno invia una sua foto nudo

Segue…. (2)

- A seguito di perquisizione per trovare la chat di whatsapp viene trovato nel computer dell'indagato A. materiale pedopornografico (su 3 diversi HD gli stessi 10 files)

Il Pubblico Ministero dott. [redacted], Sost. Procuratore della Repubblica presso Il Tribunale Di [redacted], nel procedimento penale nei confronti di [redacted] ([redacted] +1), [redacted] residente in [redacted] via [redacted] n. [redacted]

per il reato di cui all'art. 609 undecies c.p. commesso in data [redacted].

Letta la CNR avente rif. Prot. nr. [redacted] del [redacted] redatta da personale del Reparto Territoriale Carabinieri di [redacted] – [redacted] – [redacted]

Ritenuto che vi sia fondato motivo di ritenere che nella abitazione, in altri locali ed automezzi o luoghi nella disponibilità di [redacted] possano essere rinvenute fonti di prova in ordine al reato di cui sopra, nonché cose o tracce pertinenti al reato per cui si procede, nel caso specifico, telefoni cellulari, personal computer, sia in stazione fissa che portatili, notebook, netbook, hard-disk di qualsiasi formato, pendrive, supporti magnetici, ottici e video anche questi di qualsiasi formato, nonché qualunque altra documentazione relativa alle condotte per le quali si procede - **ed in particolare elementi dai quali si possa desumere la riferibilità all'indagato delle conversazioni (sms, chat, etc.) intercorse, mediante l'applicazione Whatsapp, tra quest'ultimo e la p.o. minore degli anni 18.**

A) Imputazione (3)

1. del reato previsto e punito dall'art. 600 *quater* c.p. perché consapevolmente deteneva* su due hard disk [redacted] dieci files video ritraenti minori degli anni diciotto ripresi nell'atto di compiere e subire atti sessuali espliciti e reali, nonché minori degli anni diciotto ripresi negli organi genitali per scopi sessuali.

In [redacted]

2. del reato previsto e punito dagli artt. 81 cpv, 609 *undecies* c.p. perché, con più azioni esecutive di un medesimo disegno criminoso, allo scopo di produrre materiale pornografico utilizzando la minore [redacted] e comunque di procurarsi detto materiale, nonché di compiere atti sessuali sulla stessa, la adescava carpendone la fiducia attraverso lusinghe poste in essere mediante l'utilizzo del programma Whatsapp installato sul proprio telefono cellulare e su quello della persona offesa.

B) Imputazione (4)

1. del reato previsto e punito dagli artt. 81 cpv, 609 *undecies* c.p. perché, con più azioni esecutive di un medesimo disegno criminoso, allo scopo di produrre materiale pornografico utilizzando la minore [redacted], e comunque di procurarsi detto materiale, nonché di compiere atti sessuali sulla stessa, la adescava carpendone la fiducia attraverso lusinghe poste in essere mediante l'utilizzo del programma Whatsapp installato sul proprio telefono cellulare e su quello della persona offesa.

[redacted]

2. del reato previsto e punito dall'art. 609 *quinquies* co. II c.p. perché mostrava alla minore [redacted] materiale pornografico, ed in particolare la foto dei propri genitali, al fine di indurla a compiere atti sessuali.

[redacted]

MOTIVI

[redacted], padre della minore tredicenne [redacted], ha denunciato in data [redacted] fatti di presunto adescamento della propria figlia da parte di due persone tali [redacted] (A) attraverso lo smartphone ed il social profile *whattsapp*.
L'uomo spiegava di aver notato insieme alla moglie e madre della ragazza un recente 'turbamento' complessivo nell'atteggiamento e preteso di controllare lo smartphone a lei in uso.
Forniva contestualmente alla denuncia ai Carabinieri i fogli con le trascrizioni dei messaggi scambiati con tali '[redacted] (A) ed [redacted] (B)' ed indicava i numeri di utenze relativi riportando altresì *'de relato'* quanto appreso dalla propria figlia sulla vicenda:
la ragazza aveva comunicato ai suoi interlocutori di avere compiuto 15 anni;
sul profilo del social è ritratta una fotografia della ragazza;
appena scoperte dai genitori le relazioni virtuali con i due uomini la [redacted] aveva *cancellato* alcuni dialoghi ed in particolare una foto definita *'schifosa'* inviatale da [redacted] (B)
il denunciante poi sintetizzava gli argomenti dei dialoghi rintracciati sullo smartphone e li *scaricava* su carta;
i dialoghi rimasti in memoria sono allegati alla denuncia.
I Carabinieri risalivano tramite le utenze di cui alle *chat* ai due odierni imputati titolari delle utenze.

Dopo le identificazioni dei due imputati nel mese di ottobre del 2013 venivano eseguite le perquisizioni nelle abitazioni, sequestrati e poi analizzati gli Smartphone.

In particolare, si legge nella relazione tecnica relativa agli accertamenti svolti sugli apparecchi, che sull'apparecchio di [redacted] erano ancora leggibili nel contatto su whattsapp i dialoghi con la utenza della [redacted] mentre sul databse dello smartphone all'epoca in uso all'[redacted], non erano stati rinvenuti i dialoghi con la [redacted] poiché le chat disponibili erano solo quelle dal [redacted] in poi

Quanto alla utilizzabilità delle 'trascrizioni' delle conversazioni fornite dal denunciante (padre della persona offesa dal reato, minorenne) posta in dubbio dai difensori, solo due brevi considerazioni –essendo materia già ampiamente trattata dalla giurisprudenza della Suprema Corte-.
Siamo in presenza di *dialoghi* 'registrati' nella memoria dello smart-phone della ragazzina il cui contenuto e significato, di per sé, è elemento costitutivo del reato.
La valenza probatoria è quella rappresentativa di dialoghi effettivamente avvenuti tra i soggetti e memorizzati in un 'documento' informatico; la loro trasposizione su carta, da parte del denunciante è solo una modalità di acquisizione di dati.

trascrizioni.
Sul delitto di adescamento, la recente introduzione della figura di reato ha inteso sanzionare condotte che non siano *ancora* configurabile come tentativo o la consumazione del reato-fine, ossia nel caso di specie: prostituzione minorile, pornografia minorile e poi produzione di materiale prongrafico fino alla violenza sessuale e, altrimenti si dovrà procedere solo per tali reati e non per l'adescamento, che rimarrebbe assorbito. E' quanto emerge dalla sentenza della Terza Sezione Penale della Corte di Cassazione del 20 aprile 2015, n. 16329 :"*Il delitto di adescamento di minori è punibile, in virtù della clausola di riserva "se il fatto non costituisce più grave reato", solo se non*

siano ancora configurabili gli estremi del tentativo o della consumazione del reato fine, in quanto, nell'ipotesi che quest'ultimo resti allo stadio della fattispecie tentata, la contestazione anche del delitto di cui all'art. 609-undecies cod. pen. significherebbe di fatto perseguire la stessa condotta due volte, mentre, qualora il reato fine sia consumato, la condotta di adescamento precedentemente tenuta dall'agente si risolverebbe in un antefatto non punibile. (Fattispecie in cui è stata ritenuta la configurabilità del reato di tentativo di atti sessuali con minorenne ed esclusa quella del delitto di adescamento in relazione alla condotta di imputato che, con spasmodico invio di "sms" e organizzazione di incontri spirituali o di istruzione musicale, aveva cercato di circuire ragazzi minorenni)."
Quanto alle modalità della condotta la norma offre una definizione della parla *adescamento* inteso come *qualsiasi atto volto a carpire la fiducia del minore* …anche attraverso la via telematica; tali sono le modalità utilizzate dai due imputati come è fin troppo chiaro ed agevole leggere nelle conversazioni.

Quanto alle modalità della condotta la norma offre una definizione della parla *adescamento* inteso come *qualsiasi atto volto a carpire la fiducia del minore* …anche attraverso la via telematica; tali sono le modalità utilizzate dai due imputati come è fin troppo chiaro ed agevole leggere nelle conversazioni.
Ciò detto quanto all'articolo 609 *undecies* c.p., non è necessario avuto riguardo al capo 2) contestato all'[redacted] acquisire 'visivamente' al processo l'immagine dell'organo sessuale di [redacted] in erezione, essendo sufficientemente rappresentativo ed 'indiziante' quanto detto 'spontaneamente dalla ragazza [redacted] nella conversazione sopra accennata, e quanto riferito dalla stesa al padre, come esposto in denuncia. La prova dichiarativa può senz'altro supplire a quella documentale qualora quest'ultima non sia più disponibile.

Detenzione di materiale pedopornografico: la prova dei metadati

Può invece essere condivisa la tesi difensiva di [redacted] sulla insufficiente dimostrazione del delitto di cui all'articolo [redacted]
I 10 video pedopornografica sono stati scaricati dalla pg operante dai 3 supporti informatici di [redacted] ma apprezzabili da questo GIP solo avuto riguardo soltanto alle immagini iniziali con cui sono registrati e, per la verità, non tutte chiarissime. Conclude il CT della difesa con alcune argomentazioni condivise che pongono in dubbio la *intenzionalità* e dunque il 'dolo' da paret dell'utente circa la loro acquisizione/detenzione. Innanzitutto il materiale che si possa definire obiettivamente pedopornografico è di 6 file(dei 10 incriminati) e rappresenta una mole esigua rispetto alla mole di documenti di altra natura ed ai 518 filmati di altro genere presente nei supporti; le locazioni le denominazioni e i *'metadati'* ossia le informazioni sui dati dei files, fanno supporre che si tratti ci *copie, di copie effettuate automaticamente durante una procedura di* back up, ossia la procedura di replica dei dati per salvare la memoria di un dispositivo, eseguito in modo non selettivo ma globale, senza una specifica volontà dell'utente. Infine –osserva il CT- non ci sono elementi probanti che il predetto materiale sia stato effettivamente visionato, spiegandone in modo esaustivo le ragione sulla base dell'analisi dei metadati.

Tribunale di Milano (2)

- A.B e C. sono accusati di avere detenuto foto scattate all'interno di una proprietà privata e di averle messe in vendita. A comprova dei loro rapporti e del loro intento, secondo le Procura della Repubblica, ci sono degli sms tra di loro
- A. il telefono di A è stato infatti sequestrato «per trovare le foto incriminate»- e invece sono stati estrapolati i messaggi tra lui e B. e tra lui e C.
- Dagli sms con A., C. appare a conoscenza delle foto e quindi già indagata

La P.G. sente a s.i.t. C. e:

- Le chiede la password di accesso alla posta elettronica
- Modifica la password di accesso e inserisce la propria mail quale mail di recupero password
- «congela» l'account di posta senza richiedere rogatoria

riesame

Nel verbale delle operazioni compiute a seguito del decreto di sequestro, la PG dà atto quanto segue " *interpellato in merito l'ISP competente (gorge Italia srl) per il tramite dello studio legale che segue i rapporti con l'AG dell'ISP medesimo si apprendeva che non era possibile eseguire il sequestro per difetto di giurisdizione poiché i server sui quali Google memorizza gli account dei propri utenti si trovano in territorio estero*". Come si è in precedenza riferito, il dato effettivamente emerge da uno scambio di messaggi di posta elettronica tra la squadra di Pg incaricata delle operazioni e l'ufficio legale di Google, ove si specifica, tra l'altro, che anche ai fini di un mero congelamento provvisorio dei contenuti di un account Gmail, è necessario che sia formalmente avviata da parte dell'autorità giudiziaria la procedura rogatoriale (cfr e mail del 18 gennaio 2012 ore 17,58).

Se dunque questa è la premessa operata dalla stessa Pg , è evidente che il provvedimento di sequestro emesso dal Pm non è stato in alcun modo posto in esecuzione; ed infatti, per esecuzione non può che intendersi la apposizione di un vincolo sul bene seguendo – almeno in linea generale- le modalità astrattamente previste dalla legge per l' attuazione di un provvedimento dell'autorità giudiziaria. Ove la PG – assumendo una condotta che esula del tutto dagli schemi legislativi previsti dalla normativa nazionale e internazionale per la esecuzione di un determinato provvedimento e dando atto essa stessa della impossibilità di tale esecuzione - si attivi in ogni caso al fine di assicurare la fonte di prova, tale condotta non può che essere qualificata come atto di iniziativa della polizia giudiziaria, non autonomamente impugnabile fino a che non sia intervenuto un provvedimento di convalida ad opera del PM.

Nel caso di specie la PG ha, peraltro, posto in essere un atto del tutto atipico e che in sostanza –a prescindere dal concreto intento degli operanti che era solo quello di "cautelare l'oggetto del sequestro"- si risolve (trattandosi di account di posta elettronica formalmente ancora attivo, pur se sottratto alla disponibilità della parte), come correttamente evidenziato dalla difesa, in una possibile intercettazione di flussi di comunicazione futuri (in particolare di e- mail inviate alla [redacted] da terzi non a conoscenza del provvedimento di sequestro), con conseguente snaturamento della funzione –di mera cristallizzazione di dati- propria del sequestro probatorio e violazione delle norme (art. 266 e seguenti c.p.p.) che prescrivono ben altre modalità per l'attivazione di simili operazioni di controllo ad opera dell'autorità giudiziaria. Si impone dunque su tale atto –si ripete non qualificabile e non qualificato dalla stessa Pg come esecuzione del provvedimento di sequestro oggi in esame, ma tale da imporre un autonomo vincolo sul bene- un immediato vaglio giurisdizionale ad opera del

Tribunale di Palermo (3)

- «Capo A) delitto di cui all'art. 479 c.p. aggravato dall'art. 61 nn. 2-9 c.p., per avere in concorso tra loro violato i doveri inerenti all'esercizio della pubblica funzione di Direttore Generale dell'Azienda Ospedaliera xxxxxxxxxxxxx ricoperta da F., retrodatando al 03.07.08 il provvedimento contenuto nella nota prot. n. cccccccc, in realtà predisposta il 31.07.2008, al fine di indurre in errore la Regione -------- e conferire, ad A., l'incarico a tempo determinato di dirigente responsabile del settore affari generali e legali ex art. yyyyyyyyyy, eludendo la "*sospensione di ogni procedimento amministrativo attinente il conferimento di incarichi dirigenziali* " con conseguente danno patrimoniale della Regione stessa. Fatto commesso in Palermo il 31 luglio 2008.
- N.B.: La nota (provvedimento) è stata predisposta mediante file di word poi stampata e firmata il 3 luglio 2008. Il metadato «data di creazione è del 31.7.2008

CTPM: sequestro del PC in uso e dei due precedenti

>CTPM

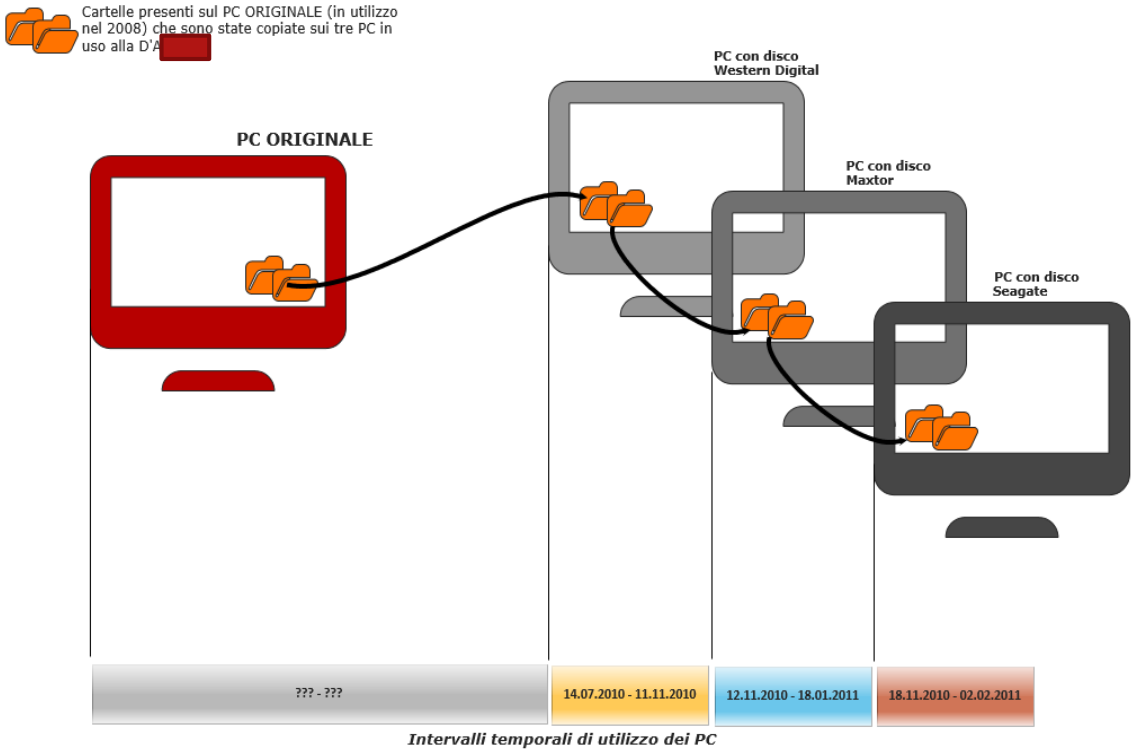
9QE24DJB

Il reperto di cui al punto a) risulta sequestrato il 2 febbraio 2011 presso la direzione generale P[redacted]i reperti di cui ai punto b) e c) risultano sequestrati il medesimo giorno, e trattasi di 2 hard disk che in passato erano installati in computer utlizzati dallo stesso personale che ha in uso il computer di cui al punto a), e che sono stati sostituiti dall'assistenza tecnica nel novembre 2010 (b) e nel gennaio 2011 (c).

Nello specifico:

- nel novembre 2010 l'hard disk S/N WCAT21939919 (b) è stato sostituito dall'hard disk S/N 9QE24DJB (c);
- il 18 gennaio 2011, l'hard disk S/N 9QE24DJB (c) é stato sostituito dall'hard disk S/N 9VMKXGMS installato nel computer al momento del sequestro (a)

> CTP



PC in uso (nel febbraio 2011 ma i fatti sono del luglio 2008)

- Operazioni identiche sui 3 pc ma NESSUNO è IL PC CON CUI è STATO SCRITTO IL FILE WORD IN ORIGINALE. Relazione del CTPM- 359 c.p.p.

Il file viene stampato e allegato in appendice alla presente relazione.

Gli orari di creazione e ultima modifica dei, così come memorizzati dal sistema operativo, coincidono, come indicato nella seguente tabella[7]:

	Created	*Modified*
1)	2010-Jul-14 11:50:37.312500 UTC	2008-Jul-31 12:25:08 UTC
2)	2010-Jul-14 11:50:37.312500 UTC	2008-Jul-31 12:25:08 UTC

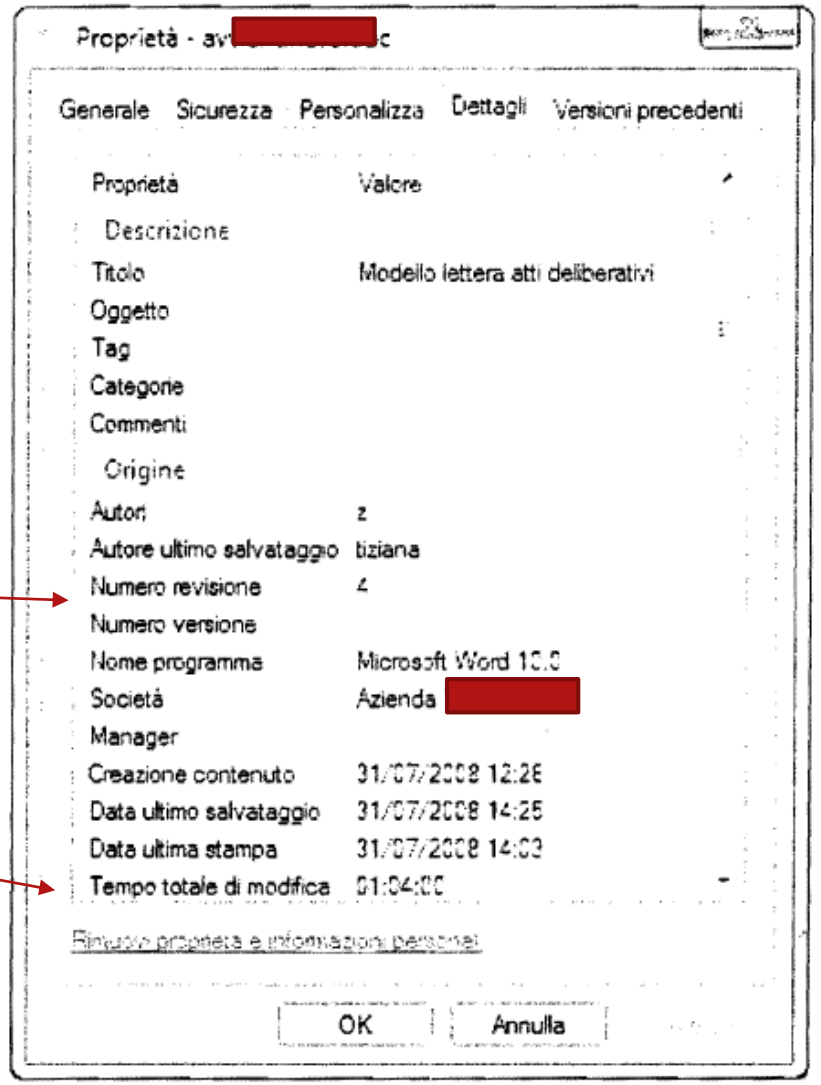
In merito ai dati sopra riportati, occorre precisare che non si tratta di dati associati direttamente al file (metadati), ma di dati gestiti dal Sistema Operativo; per tale

ragione, quando ci si trova in presenza di un file la cui data (e/o ora) di creazione è successiva alla sua data (e/o ora) di ultima modifica, la data di creazione NON indica il momento in cui il file è stato effettivamente creato, ma piuttosto specifica il momento in cui il file è stato copiato sul supporto gestito dal sistema operativo (nel caso specifico, l'hard disk in esame).

La data di ultima modifica indica invece la data e l'orario in cui il file ha subito l'ultima modifica.

Pertanto, si può affermare che il file [redacted] ha subito l'ultima modifica il giorno 31 luglio 2008 alle ore 14:25 (orario italiano)[8].

Per verificare quindi la effettiva data di creazione del file, sono stati analizzati i metadati associati a un documento Word, dati cioè che rimangono invariati anche se il file viene spostato da un supporto a un altro (ad esempio, da un hard disk a un altro). L'immagine seguente riporta le informazioni così ottenute 8in questo caso, gli orari sono già espressi secondo l'orario italiano):



Pertanto, si può affermare che il file *a[redacted].doc* è stato creato il 31 luglio 2008 alle ore 12:26 (orario italiano), e ha subito l'ultima modifica il 31 luglio 2008 alle ore 14:25 (orario italiano).

CTP (difesa) e CTU

- Il verbale di sequestro è stato redatto con il pc sequestrato
- Non c'è tra i reperti il pc originale e quindi si lavora solo su file che sono copie di backup (data installazione- versioni di office)
- Tasto destro del mouse invece di software di ricerca metadati (visualizzati solo alcuni dei metadati)
- I metadati sono modificabili
- Nel pc c'era un file con nome identico se non per una lettera generato il giorno stesso in cui si presumeva creato l'altro
- L'analisi deli metadati del file evidenzia 4 revisioni e un'ora di timing
- Le operazioni di salva con nome modificano la data di creazione di un file (save as a new document)

Tribunale minorenni di Milano (4)

- Perquisizione e sequestro di 5 telefonini
- Processo per tentato omicidio
- I difensori non vengono avvisati: perquisiamo o ci date i cellulari spontaneamente?

In Italia: quali diritti dell'indagato?

- **Indagato: ha la facoltà di non rispondere e non deve dire il vero**

Testimone: ha l'obbligo di rispondere e dire il vero

Sentito a verbale: s.i.t o interrogatorio?

Rivelare la password?

E se il cellulare è protetto?

Legione Carabinieri Lombardia

COMPAGNIA DI MILANO [redacted]
NUCLEO OPERATIVO

[redacted]

OGGETTO: Verbale di sequestro di:

- **Nr.1 cellulare** marca IPhone avente [redacted] con scheda telefonica **Wind avente nr.** [redacted]

operato a carico di: ----------

- [redacted] nato a Milano il [redacted] ivi residente in via Cascina Bianca n.8, identificato mediante C.I. nr. [redacted], rilasciata dal Comune di Milano il [redacted]

Il giorno 23/09/2017 alle ore 11:55 in Milano negli uffici del Nucleo Operativo in intestazione i sottoscritti ufficiali di P.G. Ten. [redacted] Brig. Ca. [redacted], rispettivamente Comandante ed addetto al predetto reparto, riferiscono quanto segue: ----------

"Dovendo dare esecuzione al Decreto di Perquisizione Domiciliare emesso il 19 settembre 2017 dal P. M. [redacted] nell'ambito del

[redacted] spontaneamente consegnava ai verbalizzanti quanto in oggetto meglio descritto che viene quindi posto sotto sequestro.---///

Il corpo di reato verrà trattenuto presso questi uffici a disposizione dell'A.G. mandante e per gli accertamenti tecnici "ripetibili" richiesti.----/////

Del presente verbale ne sono state redatte più copie, delle quali una sarà trasmessa alla competente Autorità Giudiziaria, una sarà conservata agli atti di questo ufficio ed una viene consegnata nelle mani dell'indagato per gli usi consentiti dalla Legge.

Il verbale viene altresì firmato dalla Signora [redacted], esercente la patria potestà del minorenne.---//

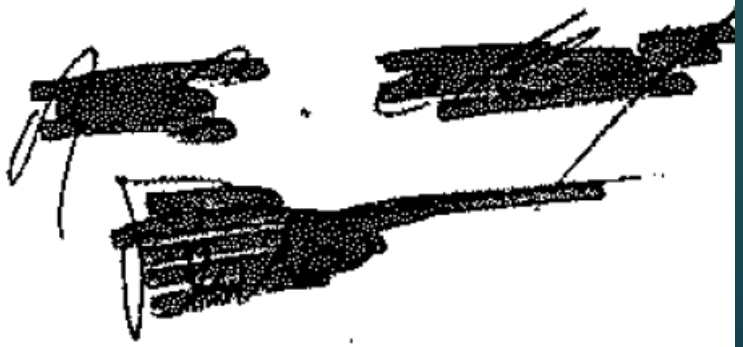
Fatto, letto, confermato e sottoscritto in data e luogo di cui sopra. ----------

L'indagato

[redacted]

Il genitore

Gli Ufficiali di P.G.



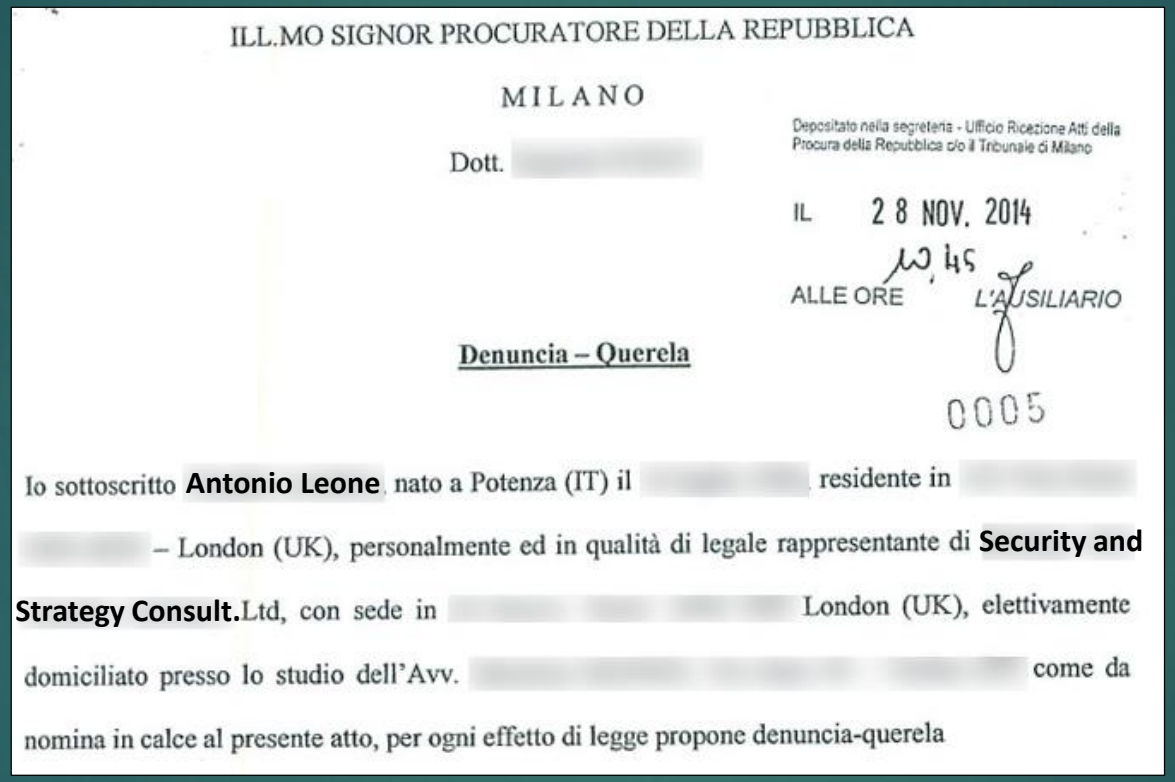
Codice sbocco : [redacted]

Codice sbocco SIH : [redacted]

Caso di studio

«come non si presentano prove elettroniche… *ma va bene lo stesso!*»

Alessandro Borra



ILL.MO SIGNOR PROCURATORE DELLA REPUBBLICA

MILANO

Dott.

Depositato nella segreteria - Ufficio Ricezione Atti della Procura della Repubblica c/o il Tribunale di Milano

IL 28 NOV. 2014

ALLE ORE 10,45

L'AUSILIARIO

Denuncia – Querela

0005

Io sottoscritto **Antonio Leone**, nato a Potenza (IT) il [redacted] residente in [redacted] – London (UK), personalmente ed in qualità di legale rappresentante di **Security and Strategy Consult.**Ltd, con sede in [redacted] London (UK), elettivamente domiciliato presso lo studio dell'Avv. [redacted] come da nomina in calce al presente atto, per ogni effetto di legge propone denuncia-querela

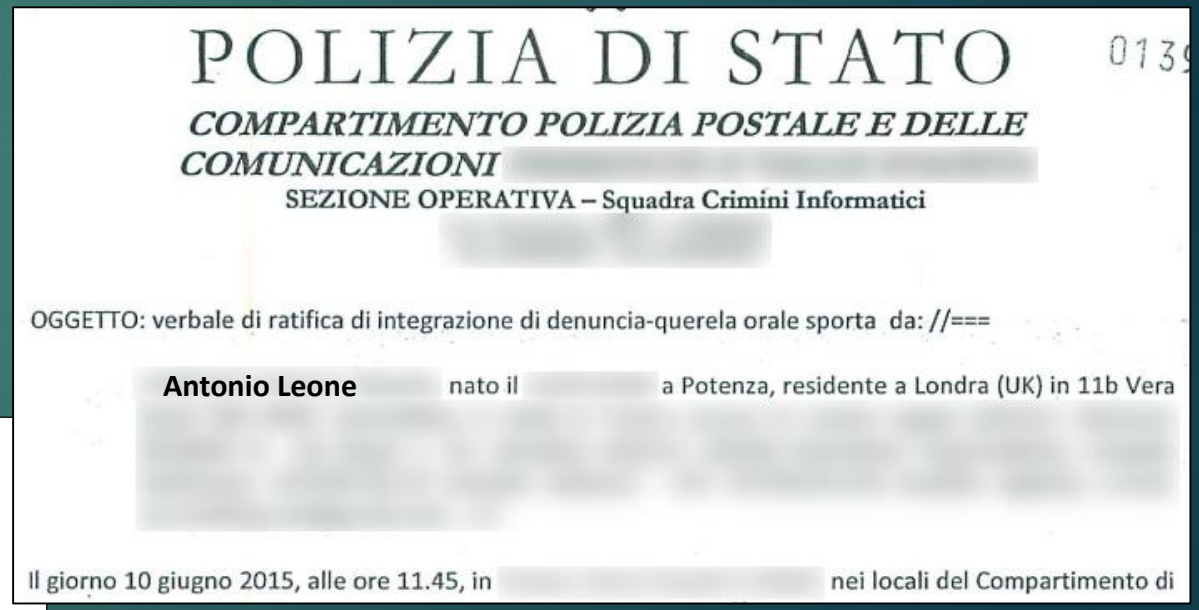
2014: denuncia-querela

- Antonio Leone, rappresentante legale 'Security and Strategy Consultancy Ltd'
- Cosimo Innocenti, … hacker!

Cosa dice di aver subito Antonio Leone:

- 1° attacco cyber a mail aziendali
- violazione di due account aziendali
- fatti avvenuti il… non si sa, ma forse tra maggio e giugno 2014. Forse ottobre…

- 2° attacco cyber a mail aziendali
- cambiate le password a due account
- fatto avvenuto a fine maggio 2015



POLIZIA DI STATO

COMPARTIMENTO POLIZIA POSTALE E DELLE COMUNICAZIONI

SEZIONE OPERATIVA – Squadra Crimini Informatici

OGGETTO: verbale di ratifica di integrazione di denuncia-querela orale sporta da: //===

Antonio Leone nato il a Potenza, residente a Londra (UK) in 11b Vera

Il giorno 10 giugno 2015, alle ore 11.45, in nei locali del Compartimento di

ATTO DI INTEGRAZIONE DELLA DENUNCIA-QUERELA DEPOSITATA IN DATA

28.11.2014

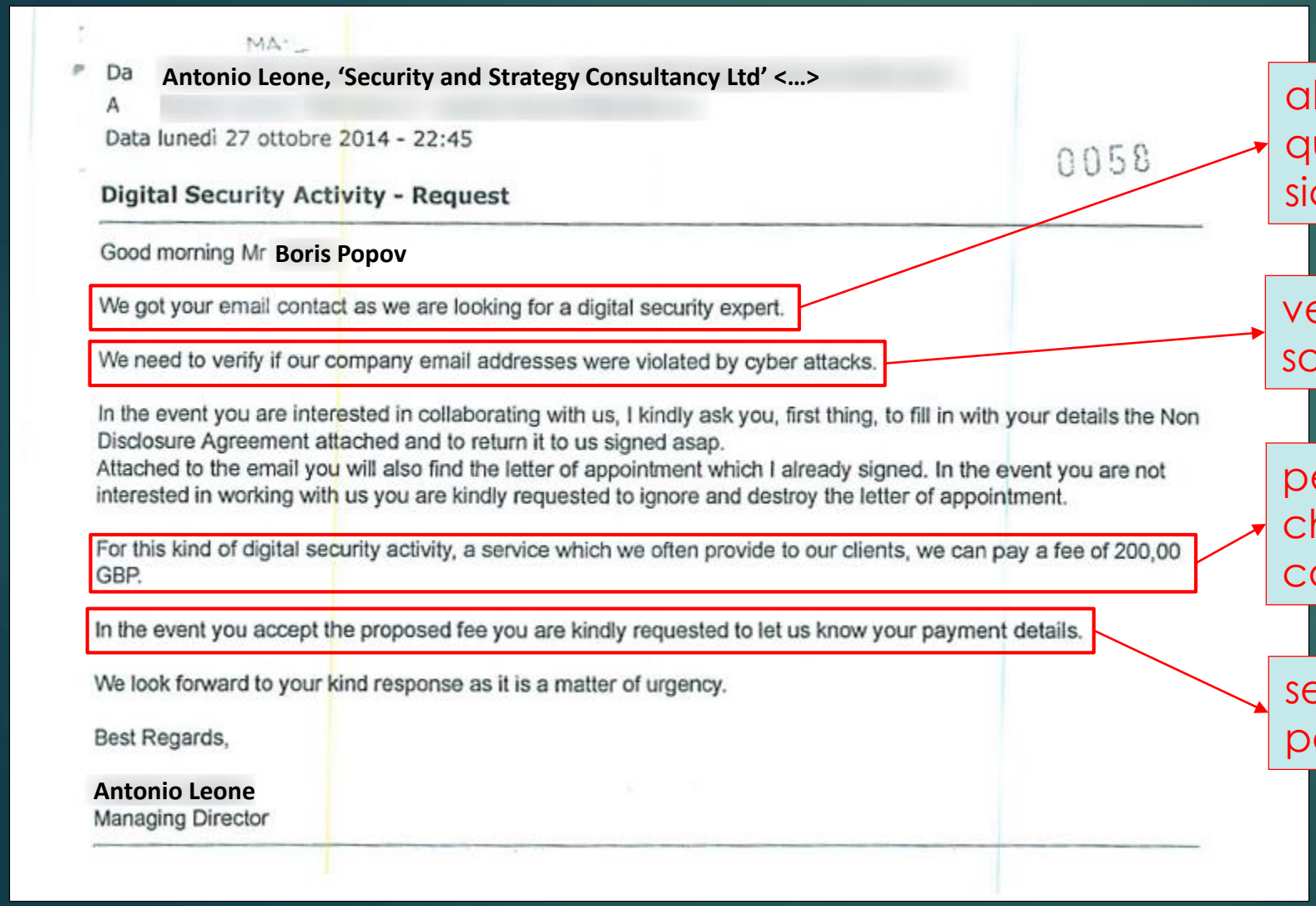
Io sottoscritto **Antonio Leone**, nato a Potenza (IT) il residente in

Cosa bisogna fare per dare evidenza di un *attacco cyber*?

- trovare un buon consulente tecnico, noto e con un buon CV
- dare un quesito preciso
- pagare… il giusto (si parla di esperto di sicurezza)
- avere una relazione tecnica ben strutturata

INDICE DEL CONTENUTO

1. trovare un buon consulente tecnico, noto e con un buon CV
2. dare un quesito preciso
3. pagare… il giusto (si parla di esperto di sicurezza)



Da **Antonio Leone, 'Security and Strategy Consultancy Ltd' <…>**
A
Data lunedì 27 ottobre 2014 - 22:45

0058

Digital Security Activity - Request

Good morning Mr **Boris Popov**

We got your email contact as we are looking for a digital security expert.

We need to verify if our company email addresses were violated by cyber attacks.

In the event you are interested in collaborating with us, I kindly ask you, first thing, to fill in with your details the Non Disclosure Agreement attached and to return it to us signed asap.
Attached to the email you will also find the letter of appointment which I already signed. In the event you are not interested in working with us you are kindly requested to ignore and destroy the letter of appointment.

For this kind of digital security activity, a service which we often provide to our clients, we can pay a fee of 200,00 GBP.

In the event you accept the proposed fee you are kindly requested to let us know your payment details.

We look forward to your kind response as it is a matter of urgency.

Best Regards,

Antonio Leone
Managing Director

abbiamo avuto il suo contatto in quanto cerchiamo un esperto di sicurezza digitale

verificare se le nostre mail aziendali sono state violate

per questo tipo di attività, un servizio che forniamo spesso ai nostri clienti, il compenso è di 200 sterline

se accetta ci fornisca i riferimenti per il pagamento

Boris Popov ??

The present agreement is dated: 27/10/2014

- **Security and Strategy Consultancy Ltd** London
  Leone Managing Director
- ***Boris Popov*** *– INSERT Address*
  ST PETERSBURG
  191025 RUSSIA

Hereafter referred to as Parties

Da **Boris Popov**
A **Antonio Leone**

Data domenica 2 novembre 2014 - 15:34

Digital Security Report

Mr **Leone**,

I send you the Digital Security Report attached
For the cost, it's OK to check which way to pick you up at your home in London

Best Regards,
--
boris popov

Digital Security

Allegato(i)

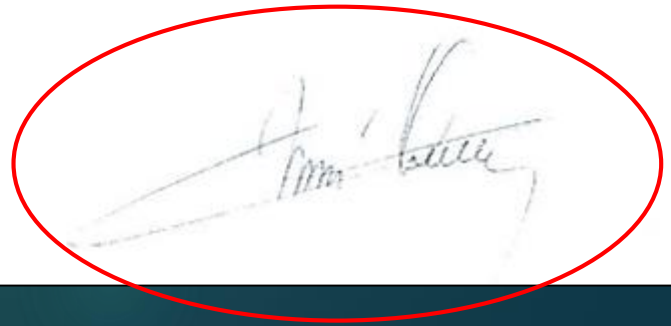
BodyPart.doc (47 Kb)
BodyPart.jpeg (327 Kb)
BodyPart.jpeg (554 Kb)
BodyPart.jpeg (291 Kb)

Digital Security Report

Appointment Received: 27/10/2014

Mr **Antonio Leone**

with reference to the Appointment Letter for the digital security activity dated 27/10/2014 signed by you, I inform you that I investigated first thing on the email account: . I will investigate also on the email account: upon payment of the first fee.



la lettera di incarico

Re: Letter of Appointment

With the present document I, the undersigned, **Antonio Leone** managing director of **Security and Strategy Cons.** Ltd appoint Mr **Popov** digital security and defense expert, for the company's digital security.

Mr **Popov**'s duty will consist in verifying and detecting any cyber attack on the following email accounts:

-

-

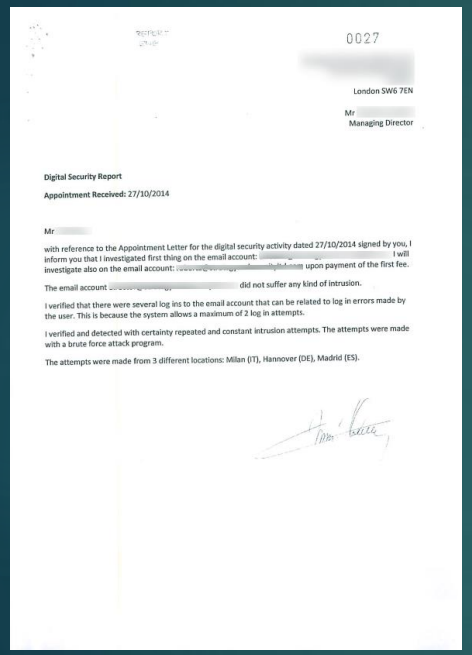
In the event any cyber attack is detected, Mr **Popov** will have the duty of investigating on the origin of the attack.

Mr **Popov** hereby agrees that during the investigations the laws of the Countries involved in the investigations will be fully respected. In particular, the UE laws, both national and transnational, regarding the subject of the investigation will be respected.

verificare e determinare qualsiasi attacco cyber a due email.
Nel caso, investigare sulle origini

la prima relazione tecnica (accesso abusivo)

5 pagine, ma 3 di allegati



0027

London SW6 7EN

Mr
Managing Director

Digital Security Report

Appointment Received: 27/10/2014

Mr

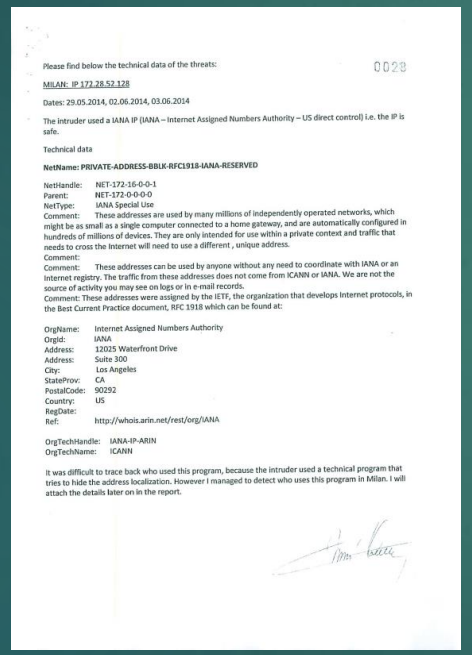
with reference to the Appointment Letter for the digital security activity dated 27/10/2014 signed by you, I inform you that I investigated first thing on the email account: . I will investigate also on the email account: upon payment of the first fee.

The email account did not suffer any kind of intrusion.

I verified that there were several log ins to the email account that can be related to log in errors made by the user. This is because the system allows a maximum of 2 log in attempts.

I verified and detected with certainty repeated and constant intrusion attempts. The attempts were made with a brute force attack program.

The attempts were made from 3 different locations: Milan (IT), Hannover (DE), Madrid (ES).



Please find below the technical data of the threats:

0028

MILAN: IP 172.28.52.128

Dates: 29.05.2014, 02.06.2014, 03.06.2014

The intruder used a IANA IP (IANA – Internet Assigned Numbers Authority – US direct control) i.e. the IP is safe.

Technical data

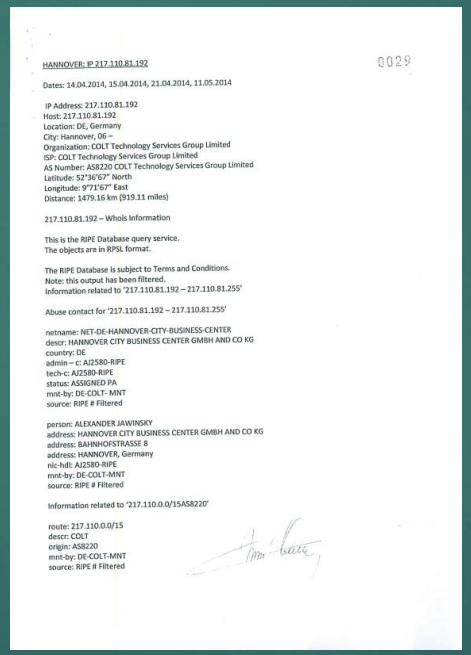
NetName: PRIVATE-ADDRESS-BBLK-RFC1918-IANA-RESERVED

NetHandle: NET-172-16-0-0-1
Parent: NET-172-0-0-0
NetType: IANA Special Use
Comment: These addresses are used by many millions of independently operated networks, which might be as small as a single computer connected to a home gateway, and are automatically configured in hundreds of millions of devices. They are only intended for use within a private context and traffic that needs to cross the Internet will need to use a different , unique address.
Comment:
Comment: These addresses can be used by anyone without any need to coordinate with IANA or an Internet registry. The traffic from these addresses does not come from ICANN or IANA. We are not the source of activity you may see on logs or in e-mail records.
Comment: These addresses were assigned by the IETF, the organization that develops Internet protocols, in the Best Current Practice document, RFC 1918 which can be found at:

OrgName: Internet Assigned Numbers Authority
OrgId: IANA
Address: 12025 Waterfront Drive
Address: Suite 300
City: Los Angeles
StateProv: CA
PostalCode: 90292
Country: US
RegDate:
Ref: http://whois.arin.net/rest/org/IANA

OrgTechHandle: IANA-IP-ARIN
OrgTechName: ICANN

It was difficult to trace back who used this program, because the intruder used a technical program that tries to hide the address localization. However I managed to detect who uses this program in Milan. I will attach the details later on in the report.



HANNOVER: IP 217.110.81.192

0029

Dates: 14.04.2014, 15.04.2014, 21.04.2014, 11.05.2014

IP Address: 217.110.81.192
Host: 217.110.81.192
Location: DE, Germany
City: Hannover, 06 –
Organization: COLT Technology Services Group Limited
ISP: COLT Technology Services Group Limited
AS Number: AS8220 COLT Technology Services Group Limited
Latitude: 52°36'67" North
Longitude: 9°71'67" East
Distance: 1479.16 km (919.11 miles)

217.110.81.192 – Whois Information

This is the RIPE Database query service.
The objects are in RPSL format.

The RIPE Database is subject to Terms and Conditions.
Note: this output has been filtered.
Information related to '217.110.81.192 – 217.110.81.255'

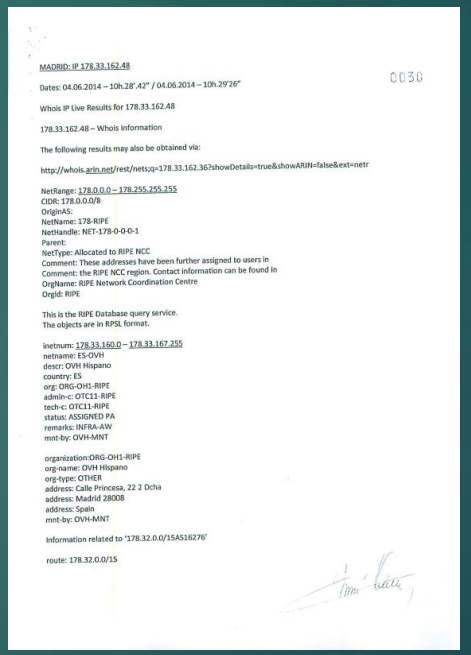
Abuse contact for '217.110.81.192 – 217.110.81.255'

netname: NET-DE-HANNOVER-CITY-BUSINESS-CENTER
descr: HANNOVER CITY BUSINESS CENTER GMBH AND CO KG
country: DE
admin – c: AJ2580-RIPE
tech-c: AJ2580-RIPE
status: ASSIGNED PA
mnt-by: DE-COLT- MNT
source: RIPE # Filtered

person: ALEXANDER JAWINSKY
address: HANNOVER CITY BUSINESS CENTER GMBH AND CO KG
address: BAHNHOFSTRASSE 8
address: HANNOVER, Germany
nic-hdl: AJ2580-RIPE
mnt-by: DE-COLT-MNT
source: RIPE # Filtered

Information related to '217.110.0.0/15AS8220'

route: 217.110.0.0/15
descr: COLT
origin: AS8220
mnt-by: DE-COLT-MNT
source: RIPE # Filtered



MADRID: IP 178.33.162.48

0030

Dates: 04.06.2014 – 10h.28'.42" / 04.06.2014 – 10h.29'26"

Whois IP Live Results for 178.33.162.48

178.33.162.48 – Whois Information

The following results may also be obtained via:

http://whois.arin.net/rest/nets;q=178.33.162.36?showDetails=true&showARIN=false&ext=netr

NetRange: 178.0.0.0 – 178.255.255.255
CIDR: 178.0.0.0/8
OriginAS:
NetName: 178-RIPE
NetHandle: NET-178-0-0-0-1
Parent:
NetType: Allocated to RIPE NCC
Comment: These addresses have been further assigned to users in
Comment: the RIPE NCC region. Contact information can be found in
OrgName: RIPE Network Coordination Centre
OrgId: RIPE

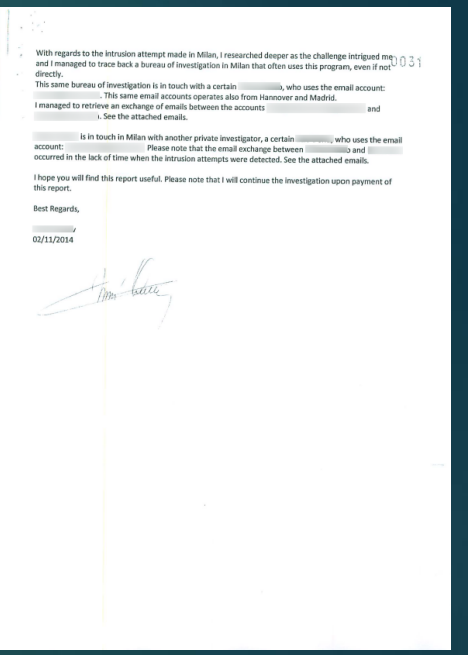
This is the RIPE Database query service.
The objects are in RPSL format.

inetnum: 178.33.160.0 – 178.33.167.255
netname: ES-OVH
descr: OVH Hispano
country: ES
org: ORG-OH1-RIPE
admin-c: OTC11-RIPE
tech-c: OTC11-RIPE
status: ASSIGNED PA
remarks: INFRA-AW
mnt-by: OVH-MNT

organization:ORG-OH1-RIPE
org-name: OVH Hispano
org-type: OTHER
address: Calle Princesa, 22 2 Dcha
address: Madrid 28008
address: Spain
mnt-by: OVH-MNT

Information related to '178.32.0.0/15AS16276'

route: 178.32.0.0/15



0031

With regards to the intrusion attempt made in Milan, I researched deeper as the challenge intrigued me and I managed to trace back a bureau of investigation in Milan that often uses this program, even if not directly.
This same bureau of investigation is in touch with a certain , who uses the email account: . This same email accounts operates also from Hannover and Madrid.
I managed to retrieve an exchange of emails between the accounts and . See the attached emails.

is in touch in Milan with another private investigator, a certain , who uses the email account: Please note that the email exchange between and occurred in the lack of time when the intrusion attempts were detected. See the attached emails.

I hope you will find this report useful. Please note that I will continue the investigation upon payment of this report.

Best Regards,

02/11/2014

la prima relazione tecnica

Please find below the technical data of the threats:

0028

MILAN: IP

Dates: 29.05.2014, 02.06.2014, 03.06.2014

The intruder used a IANA IP (IANA – Internet Assigned Numbers Authority – US direct control) i.e. the IP is safe.

Technical data

NetName: PRIVATE-ADDRESS-BBLK-RFC1918-IANA-RESERVED

NetHandle: NET-172-16-0-0-1
Parent: NET-172-0-0-0-0
NetType: IANA Special Use
Comment: These addresses are used by many millions of independently operated networks, which might be as small as a single computer connected to a home gateway, and are automatically configured in hundreds of millions of devices. They are only intended for use within a private context and traffic that needs to cross the Internet will need to use a different , unique address.
Comment:
Comment: These addresses can be used by anyone without any need to coordinate with IANA or an Internet registry. The traffic from these addresses does not come from ICANN or IANA. We are not the source of activity you may see on logs or in e-mail records.
Comment: These addresses were assigned by the IETF, the organization that develops Internet protocols, in the Best Current Practice document, RFC 1918 which can be found at:

OrgName: Internet Assigned Numbers Authority
OrgId: IANA
Address: 12025 Waterfront Drive
Address: Suite 300
City: Los Angeles
StateProv: CA
PostalCode: 90292
Country: US
RegDate:
Ref: http://whois.arin.net/rest/org/IANA

OrgTechHandle: IANA-IP-ARIN
OrgTechName: ICANN

It was difficult to trace back who used this program, because the intruder used a technical program that tries to hide the address localization. However I managed to detect who uses this program in Milan. I will attach the details later on in the report.

L' account di posta elettronica non ha subito alcun tipo di intrusione.

Ho verificato che ci sono stati diversi accessi che sono attribuibili ad errori da parte dell' utente , in quanto il sistema di protezione acconsente i tentativi di accesso alla casella di posta per un massimo di 2 volte.

Ho verificato e ho constatato con sicurezza dei tentativi di intrusione ripetuti e costanti fatti attraverso un programma di attacco denominato "brute force".

I tentativi di intrusione sono stati fatti da 3 località diverse: Milano (IT), Hannover (DE), Madrid (ES).

It was difficult to trace back who used this program, because the intruder used a technical program that tries to hide the address localization. However I managed to detect who uses this program in Milan. I will attach the details later on in the report.

E' stato difficile risalire a chi ha utilizzato questo programma, in quanto si tratta di un programma tecnico utilizzato per tentare di nascondere la localizzazione dell' indirizzo. Sono comunque riuscito ad individuare chi usa questo programma a Milano. Maggiori dettagli seguiranno in questo report.

la prima relazione tecnica (accesso abusivo)

Per quanto riguarda il tentativo di intrusione fatto a Milano, ho approfondito perché mi sembrava una sfida e sono riuscito a risalire ad un' agenzia investigativa di Milano che spesso utilizza questo programma anche se non direttamente.
La stessa agenzia investigativa è in contatto con un tale **Cosimo Innocenti** che utilizza l' account di posta elettronica: **C.Innocenti@posta.it** Questo indirizzo di posta elettronica risulta operare anche da Hannover e Madrid.
Sono riuscito a recuperare uno scambio di email tra gli indirizzi di **info@investigatore-milano.it** e **C.Innocenti@posta.it**. Si prega di vedere le email allegate.

Cosimo Innocenti è in contatto a Milano con un altro investigatore privato, tale **Ugo Ughi** i, il quale utilizza l' indirizzo email: **U.Ughi@posta.it** . Si prega di notare che lo scambio di email tra **Innocenti** ed **Ughi** è avvenuto nel periodo di tempo durante il quale sono stati riscontrati i tentativi di intrusione. Si prega di vedere le email allegate.

Spero che questo report ti sia utile. Ti prego di prendere nota del fatto che procederò nel lavoro dopo aver ricevuto il pagamento per questo report.

Cordiali Saluti,

Popov
02/11/2014

recuperate 3 mail
tra Cosimo Innocente
e due investigatori

addendum alla prima relazione tecnica (accesso abusivo)

L' account di posta elettronica [redacted] non ha subito alcun tipo di intrusione.

Ho verificato che ci sono stati diversi accessi che sono attribuibili ad errori da parte dell' utente , in quanto il sistema di protezione acconsente i tentativi di accesso alla casella di posta per un massimo di 2 volte.

Ho verificato e ho constatato con sicurezza dei tentativi di intrusione ripetuti e costanti fatti attraverso un programma di attacco denominato "brute force".

I tentativi di intrusione sono stati fatti da 3 località diverse: Milano (IT), Hannover (DE), Madrid (ES).

2

Dear Mr. **Antonio Leone**

THIS IS A DIGITAL SECURITY ALERT

Upon your request I carried out new and deeper researches.

As a result I detected without any doubt that your email ad[redacted] was hacked.

The introders accessed your email account on October 27 2014 and made a beck of of email account.

The hacker operates from the same IP address in Hannover.

Please see the technical data attached.

I remain at your disposal.

Regards

Popov

Digital Security Report

IP: 217.1[redacted]
Location: Hannover (D)

O.S.: Linux

Login attack:

<form name="login" action="login.php" method="post"> Username: <input type="text" name="user"> Password: <input type="password" name="password"> </form>

Start Time: Mon Oct 27 2014 - H 23:32

URL BASE: HTTP://webmaildominiold.aruba.it/

WORDLIST FILES: wordlists/common.txt

SERVER BANNER: lighttpd/1.4.15

(location: "-size 345)

Gererating Wordlist....

Generated Words:838

....Scanning URL: http://webmaildominiold.aruba.it/----

FOUND: http://webmaildominiold .aruba.it/cgi-bin/webmail.cgi?
cmd=reload_mail&utoken=[redacted]

(***)DIRECTORY (*-Performed

X- Hacked : by217.[redacted] with Brute Force Attack SMTP id ep1mr170193073vb.33.1408997328023;

Path: <[redacted]>.aruba.it (smtpcg2.aruba.it. [62.149.158.232])

by mx.google.com with ESMTP id y1Csi1E39280vww.52.2014.10.27.13.08.47

SPF: none (google.com: [redacted] does not designate permitted sender hosts) client-ip=62.149.158.232;

[redacted] [62.149.158.90]) by smtpcmd02.ad.aruba.it with bizsmtp id j88n1e0021xJdJu0188nrg; Mon, 27 Oct 2014 23:16:45

-Id: <NAVPAN$35FB5F2D7F286F94B8F007A5052A309C@[redacted]>

Data transfer executed successfully

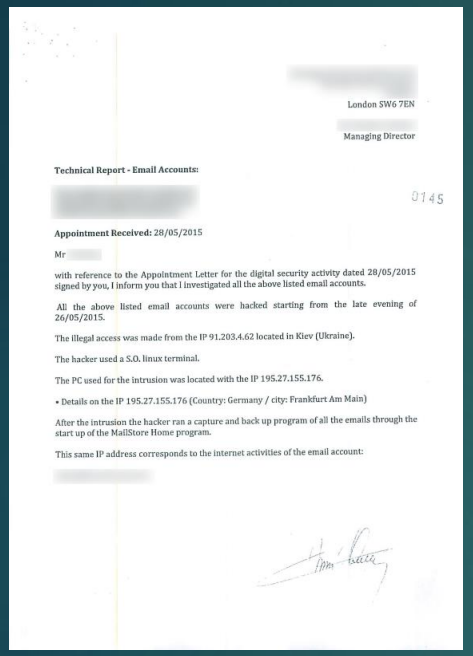
Best Regards,

Boris Popov
Digital **Security**

30/11/2014

la seconda relazione tecnica (violazione di 3 account di posta aziendali)

5 pagine, 1 solo allegato



[redacted]

London SW6 7EN

Managing Director

Technical Report - Email Accounts:

[redacted] 0145

Appointment Received: 28/05/2015

Mr [redacted]

with reference to the Appointment Letter for the digital security activity dated 28/05/2015 signed by you, I inform you that I investigated all the above listed email accounts.

All the above listed email accounts were hacked starting from the late evening of 26/05/2015.

The illegal access was made from the IP 91.203.4.62 located in Kiev (Ukraine).

The hacker used a S.O. linux terminal.

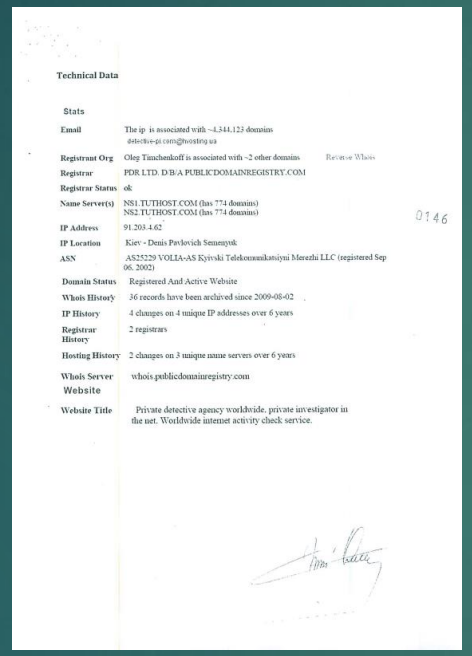
The PC used for the intrusion was located with the IP 195.27.155.176.

• Details on the IP 195.27.155.176 (Country: Germany / city: Frankfurt Am Main)

After the intrusion the hacker ran a capture and back up program of all the emails through the start up of the MailStore Home program.

This same IP address corresponds to the internet activities of the email account:

[redacted]

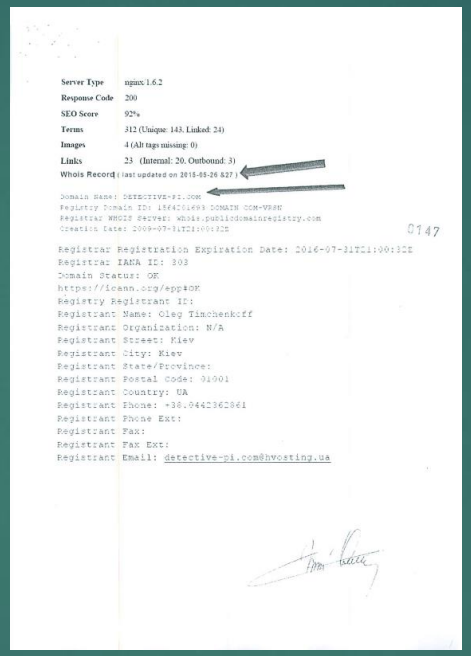


Technical Data

Stats

Email	The ip is associated with ~4,344,123 domains detective-pi.com@hvosting.ua
Registrant Org	Oleg Timchenkoff is associated with ~2 other domains Reverse Whois
Registrar	PDR LTD. D/B/A PUBLICDOMAINREGISTRY.COM
Registrar Status	ok
Name Server(s)	NS1.TUTHOST.COM (has 774 domains) NS2.TUTHOST.COM (has 774 domains)
IP Address	91.203.4.62
IP Location	Kiev - Denis Pavlovich Semenyuk
ASN	AS25229 VOLIA-AS Kyivski Telekomunikasiyni Merezhi LLC (registered Sep 06, 2002)
Domain Status	Registered And Active Website
Whois History	36 records have been archived since 2009-08-02
IP History	4 changes on 4 unique IP addresses over 6 years
Registrar History	2 registrars
Hosting History	2 changes on 3 unique name servers over 6 years
Whois Server	whois.publicdomainregistry.com
Website	
Website Title	Private detective agency worldwide. private investigator in the net. Worldwide internet activity check service.

0146

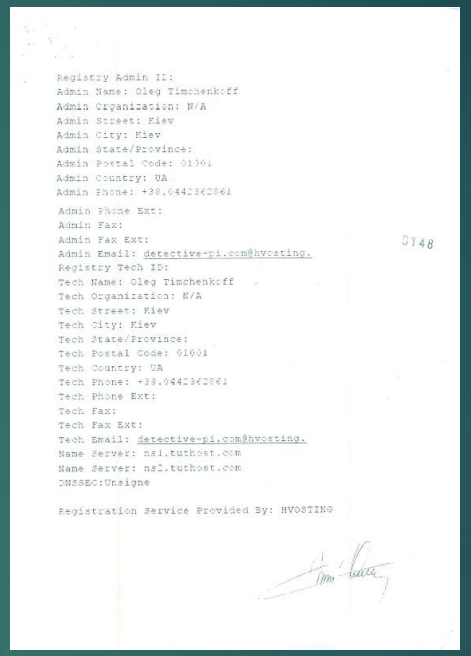


Server Type	nginx 1.6.2
Response Code	200
SEO Score	92%
Terms	312 (Unique: 143, Linked: 24)
Images	4 (Alt tags missing: 0)
Links	23 (Internal: 20, Outbound: 3)
Whois Record	(last updated on 2015-05-26 827)

Domain Name: DETECTIVE-PI.COM
Registry Domain ID: 1854201693_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.publicdomainregistry.com
Creation Date: 2009-07-31T21:00:32Z

0147

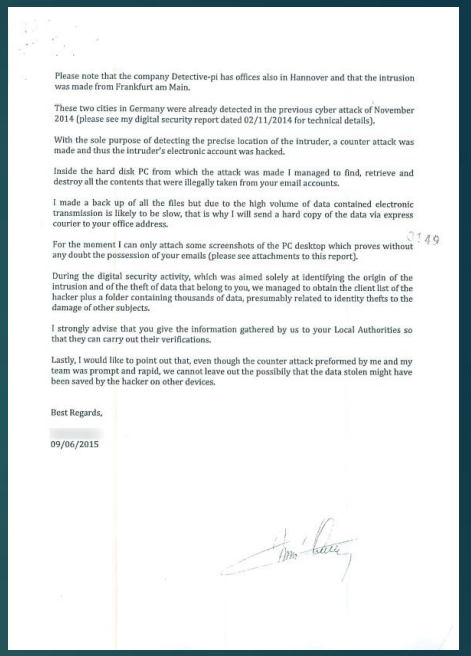
Registrar Registration Expiration Date: 2016-07-31T21:00:32Z
Registrar IANA ID: 303
Domain Status: OK
https://icann.org/epp#OK
Registry Registrant ID:
Registrant Name: Oleg Timchenkoff
Registrant Organization: N/A
Registrant Street: Kiev
Registrant City: Kiev
Registrant State/Province:
Registrant Postal Code: 01001
Registrant Country: UA
Registrant Phone: +38.0442362861
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: detective-pi.com@hvosting.ua



Registry Admin ID:
Admin Name: Oleg Timchenkoff
Admin Organization: N/A
Admin Street: Kiev
Admin City: Kiev
Admin State/Province:
Admin Postal Code: 01001
Admin Country: UA
Admin Phone: +38.0442362861
Admin Phone Ext:
Admin Fax:
Admin Fax Ext:
Admin Email: detective-pi.com@hvosting.
Registry Tech ID:
Tech Name: Oleg Timchenkoff
Tech Organization: N/A
Tech Street: Kiev
Tech City: Kiev
Tech State/Province:
Tech Postal Code: 01001
Tech Country: UA
Tech Phone: +38.0442362861
Tech Phone Ext:
Tech Fax:
Tech Fax Ext:
Tech Email: detective-pi.com@hvosting.
Name Server: ns1.tuthost.com
Name Server: ns2.tuthost.com
DNSSEC:Unsigne

Registration Service Provided By: HVOSTING

0148



Please note that the company Detective-pi has offices also in Hannover and that the intrusion was made from Frankfurt am Main.

These two cities in Germany were already detected in the previous cyber attack of November 2014 (please see my digital security report dated 02/11/2014 for technical details).

With the sole purpose of detecting the precise location of the intruder, a counter attack was made and thus the intruder's electronic account was hacked.

Inside the hard disk PC from which the attack was made I managed to find, retrieve and destroy all the contents that were illegally taken from your email accounts.

I made a back up of all the files but due to the high volume of data contained electronic transmission is likely to be slow, that is why I will send a hard copy of the data via express courier to your office address.

For the moment I can only attach some screenshots of the PC desktop which proves without any doubt the possession of your emails (please see attachments to this report).

During the digital security activity, which was aimed solely at identifying the origin of the intrusion and of the theft of data that belong to you, we managed to obtain the client list of the hacker plus a folder containing thousands of data, presumably related to identity thefts to the damage of other subjects.

I strongly advise that you give the information gathered by us to your Local Authorities so that they can carry out their verifications.

Lastly, I would like to point out that, even though the counter attack preformed by me and my team was prompt and rapid, we cannot leave out the possibly that the data stolen might have been saved by the hacker on other devices.

Best Regards,

[redacted]

09/06/2015

0149

- verifica dell'accesso abusivo: da Kiev tramite un PC sito a Francoforte
- l'attaccante ha fatto backup di tutte le mail
- controattacco: è entrato nel PC dell'hacker, ne ha fatto backup e ha cancellato i dati
- ha trovato elenco clienti dell'hacker, tra cui compare… Cosimo Innocenti!

la seconda relazione tecnica (violazione di 3 account di posta aziendali)

Incarico ricevuto: 28/05/2015

Egr. Sig. **Leone**

Con riferimento alla lettera di incarico per la sicurezza digitale datata 28/05/2015 e da lei firmata, la informo che ho provveduto ad analizzare gli indirizzi di posta elettronica a sopra elencati.

Tutti gli indirizzi di posta elettronica sopra indicati sono stati oggetto di intrusione a partire dalla tarda sera del 26/05/2015.

La forzatura è avvenuta dall' indirizzo IP 91.2 localizzato a Kiev (Ucraina).

L' hacker ha utilizzato un terminale S.O. linux.

Il Personal Computer usato durante l' intrusione è stato localizzato con l' indirizzo IP 195.2

• Dettagli sull' indirizzo IP 195.2 (Paese: Germania / città: Francoforte sul Meno)

Dopo l' intrusione l' hacker ha avviato un programma di cattura e di back up di tutte le email tramite l' avvio del programma MailStore Home.

Questo medesimo indirizzo IP corrisponde alle attività telematiche dell' indirizzo di posta elettronica:

CCCP-Investigator

pagina 1

Si prega di notare che la società **CCCP-Inv.** ha sede anche ad Hannover e che l' accesso è stato eseguito da Francoforte sul Meno.

Queste due città della Germania erano già state individuate nel precedente attacco informatico di Novembre 2014 (si prega di vedere il report di sicurezza digitale da me stilato, datato 02/11/2015 per i dettagli tecnici).

Al solo fine di stabilire l' esatta localizzazione dell' intrusione, è stato eseguito un contro attacco e quindi è stata violato l' account elettronico dell' hacker.

All' interno della memoria del computer dal quale era provenuto l'attacco informatico sono riuscito a trovare, recuperare e distruggere tutto il materiale che era stato sottratto illegalmente dai vostri indirizzi di posta elettronica.

Durante l' attività di sicurezza digitale che era indirizzata esclusivamente ad identificare l' origine dell' intrusione e la provenienza del furto dei dati di vostra proprietà, siamo riusciti a recuperare la lista dei clienti dell' hacker e anche una cartella contenente migliaia di dati, presumibilmente relativi a furti di identità a danno di altri soggetti.

Per il momento sono in grado di allegare solamente alcune fotografie del desktop del computer, le quali dimostrano inconfutabilmente il possesso delle vostre email (si prega di vedere gli allegati a questo report).

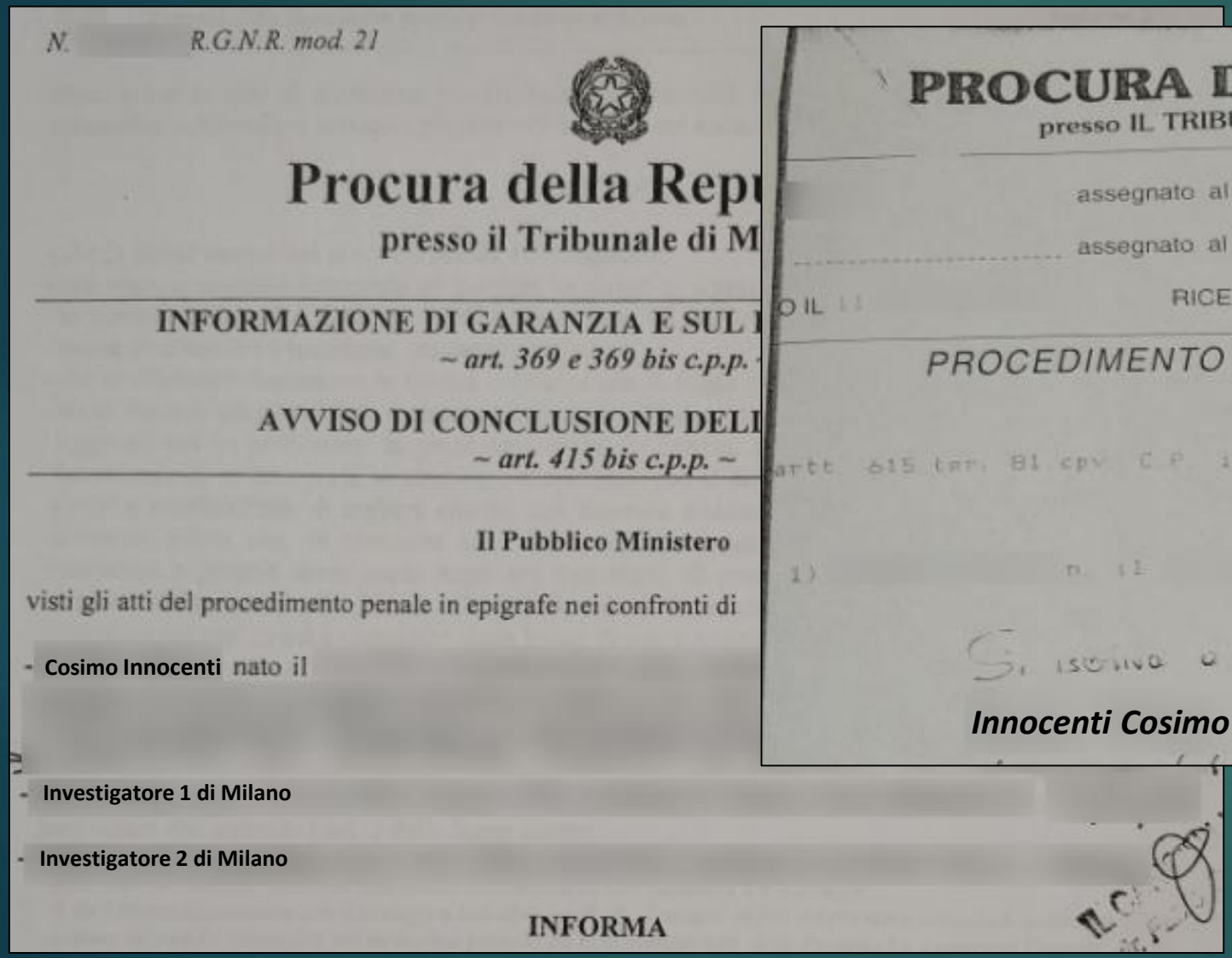
pagina 5

allegato

CONTACT LIST CLIENT

Name	Email Addr	Home Tel#	Mp#	Ofc Tel#
Cosimo Innocenti	C.Innocenti@posta.it			

sarà mica una cosa seria… o no?



N. R.G.N.R. mod. 21

Procura della Repu

presso il Tribunale di M

INFORMAZIONE DI GARANZIA E SUL

~ art. 369 e 369 bis c.p.p. ~

AVVISO DI CONCLUSIONE DELL

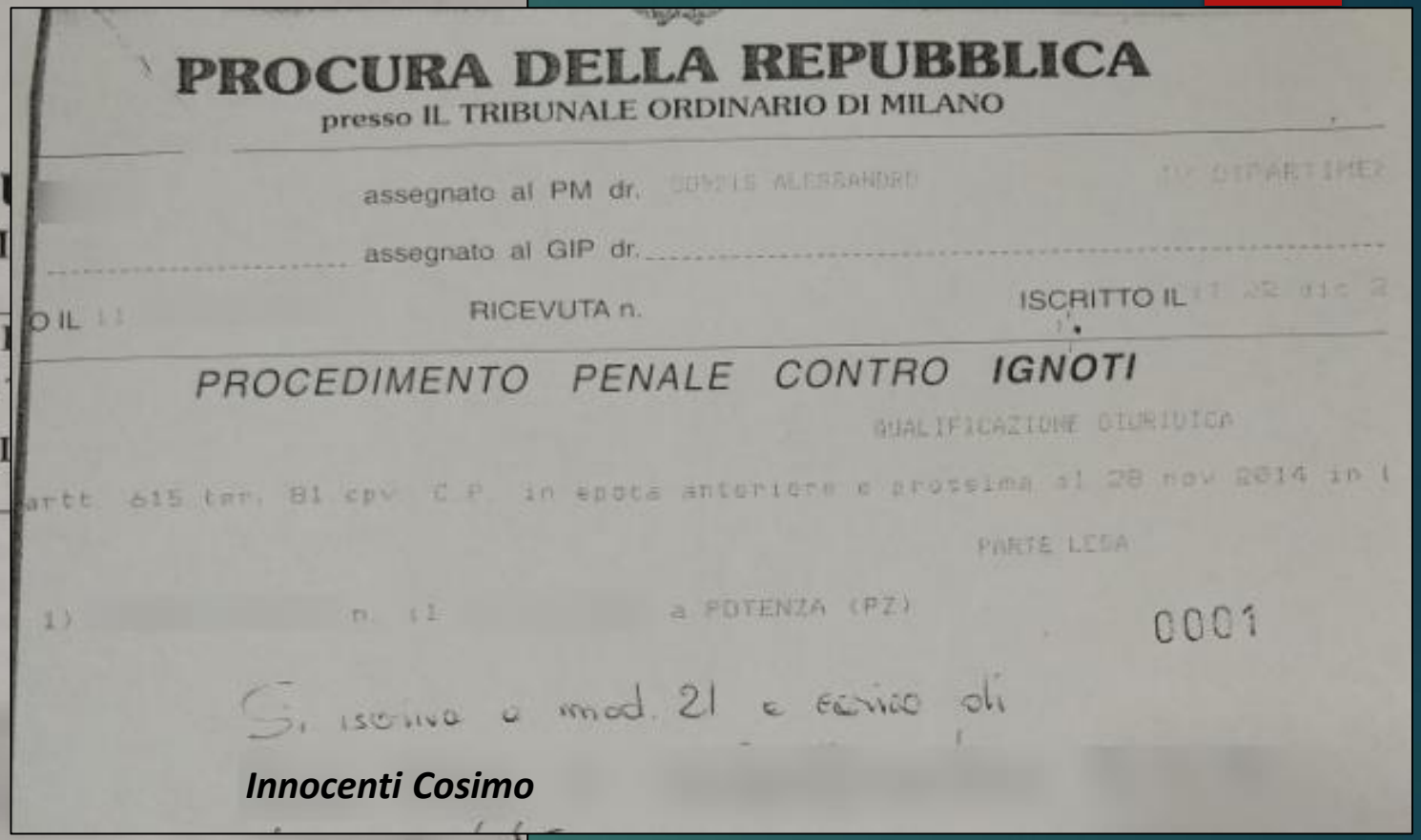
~ art. 415 bis c.p.p. ~

Il Pubblico Ministero

visti gli atti del procedimento penale in epigrafe nei confronti di

- Cosimo Innocenti nato il
- Investigatore 1 di Milano
- Investigatore 2 di Milano

INFORMA



PROCURA DELLA REPUBBLICA

presso IL TRIBUNALE ORDINARIO DI MILANO

assegnato al PM dr.

assegnato al GIP dr.

RICEVUTA n.

ISCRITTO IL

PROCEDIMENTO PENALE CONTRO IGNOTI

QUALIFICAZIONE GIURIDICA

PARTE LESA

a POTENZA (PZ)

0001

S. iscrivo a mod. 21 e cetera gli

Innocenti Cosimo

cosa è successo?

1: ah, l'informatica questa sconosciuta

2: Cosimo è un truffatore 'noto' e deve dei soldi ad Alberto Leone…