COMPUTER FORENSICS

FORENSICS DATA SCIENCE

**DOTT. MARZADURI MARCO ROBERTO M.**

# CONFERIMENTO MANDATO E QUESITO PERITALE FORENSE ACQUISIZIONE PEC FALSIFICATE E DIMOSTRAZIONE VULNERABILITÀ ARUBA PEC S.P.A.

**Nell'interesse del Dott. (coperto da privacy)**

# Marco Roberto Maria Marzaduri

DOTTORE IN SCIENZE DELL'INFORMAZIONE.

COMPUTER FORENSICS ANALYST - CERTIFIED DATA SCIENTIST

Microsoft Partner Network ID 2129435

Microsoft Competency Network Infrastructure Solutions.

Microsoft Certification ID: 258760. Certifications: MCT A., MCSA 2008, MCSA 2016-2020, MCSE, MCTS, MCP+I, MCP.

#6 Certification in Microsoft Professional Program for Data Science

Information Technology Infrastructure Library Certified.

---

**DOMICILIAZIONE INCARICO**

**Ragione Sociale**:

**(ITLIA)** Studio Marzaduri Dr. Marco R. – P.I. 05782300874

**(MALTA)** Studio Marzaduri Dr. Marco R. – P.I. MT24305614

Tel e Fax: +39 06 5655 7374 and E-mail: marco@marzaduri.com

Posta elettronica certificata PEC: dott.marzaduri@pec.it

Table of Contents

# **PARTE PRIMA** INTRODUZIONE

## LA CONSULENZA TECNICA

- **La consulenza tecnica o una relazione tecnica in formato pdf e pdf firmato digitalmente dal CT. o allegato E01 con i files richiesti e relativa impronta hash.**

## PRINCIPI GENERALI

Il quesito peritale ha guidato il CTP nella scelta delle più appropriate tecnologie hardware e software le quali sono state configurate, preventivamente testate ed infine utilizzate, rispettando le indicazioni del costruttore ed osservando le migliori pratiche forensi con particolare attenzione alle indicazioni contenute nel documento *Data Protection and Cyber crime Division - Council of Europe*.

Invariabilmente, ogni sistema informatico può contenere dati privati che sono irrilevanti per l'indagine ma confidenziali, privati e forse caratterizzati da privilegi legali; ben adempiendo alla disposizione *n.46/2008 del Garante della privacy*, il CT ha applicato tutte **misure di protezione** necessarie a partire dalla conservazione in cassaforte ignifuga dei dati reperti in ambiente video sorvegliato con due telecamere (di elevata qualità costruttiva) e due differenti sistemi di allarme.

# IL METODO DI LAVORO

Il CTP, rispettando le *best practices* e la normativa vigente, si è collegato alla PEC ARUBA del Dott. X (Coperto da Privacy), identificata da **dott.(Coperto da Privacy)@pec.it**, tramite la webapp Webmail.

La autenticazione è stata eseguita inserendo le credenziali fornite dallo stesso Dott. (Coperto da Privacy).

Dopo aver verificato con una ispezione generale la appartenenza della email allo stesso Dott. (Coperto da Privacy), si è proceduto alla estrazione di una copia esatta dei messaggi sospetti. I messaggi sono stati anche oggetti di analisi forense e autenticazione hash.

Al termine della operazione il Dott. (Coperto da Privacy) è stato invitato a cambiare subito la password di accesso alla propria PEC. Il Dott. (Coperto da Privacy) mi ha confermato con email di aver provveduto al cambio della password, esonerandomi da ogni responsabilità

## IL METODO SCIENTIFICO

Il Metodo adottato dal CT è il Metodo Scientifico del quale si precisano alcuni punti importanti tenuti in grande riguardo:

- Le *proposizioni logiche,* alle quali viene richiesto di attribuire una *costante logica* (*vero, falso),* sono applicate in ambiti ristretti come in quello della linguistica, dei linguaggi di programmazione, della ontologia informatica, della insiemistica, della matematica e più in generale ove è possibile rispondere con certezza usando una operazione di confronto, di accertamento della esistenza, un ragionamento deduttivo o induttivo.
- Il concetto di *certezza,* associato per convenzione alle costanti logiche *vero* o *falso*, dipende dalla corretta definizione di un test logico e dalla possibilità che tale test si possa applicare ai dati in esame. Per tale ragione si ritiene corretto rispondere con certezza a quesiti come: *" il numero di telefono dello smartphone dell'indagato è uguale a quello riportato negli atti di indagine*"?
  Non è corretto rispondere con certezza a quesiti come: "il messaggio di errore SD Card Error, significa che l'utente ha rimosso la scheda dallo SmartPhone?".
  Nel primo caso infatti il confronto per uguaglianza tra due numeri è possibile e la risposta può essere solo Vero o Falso. Nel secondo caso non è invece possibile stabilire una correlazione certa, uno ad uno, tra un messaggio generico di sistema ed un fatto accaduto nel mondo reale, a meno di prove di laboratorio che forniranno un dato statistico e circoscritto a condizioni ben precisate.
- Si deve distinguere *probabilità* da *possibilità* di un evento: un evento che si verifica e si può osservare è probabile altrimenti è possibile in teoria (o in potenza). Ad esempio è possibile che il sole possa esplodere ma nessuno oggi se ne preoccuperà perché è un evento non probabile.
- Un evento potrebbe essere *possibile o probabile* anche in base ad una congettura a priori.
- Quando la probabilità di un evento, ad esempio numerico, dipende dalla complessità computazionale della funzione matematica che lo genera, potremmo dover decidere se usare il termine possibile o probabile.
  - Al crescere della complessità computazionale, un evento matematico come il risultato di una funzione di calcolo potrebbe passare da probabile a non probabile ma in teoria possibile. Nella scienza forense è il caso dei codici Hash delle *copie*

*forensi*; Al crescere della complessità matematica scelta nel calcolo (MD5➐SHA1➐SHA256) oggigiorno possiamo dire, con differente grado di certezza, che "due files A e B hanno lo stesso identico contenuto se e solo se hanno lo stesso codice Hash". Sappiamo infatti che:

- ✦ È davvero poco probabile che nel mondo reale si possano trovare due file differenti con uguale codice MD5 data la elevata complessità di calcolo.
- ✦ È davvero altamente improbabile che si possano trovare due file differenti con uguale codice SHA1, data la elevatissima complessità.
- ✦ È certamente non probabile che si possano trovare due file differenti con uguale codice SHA256, data la estremamente elevata complessità.

- L'Euristica è parte dell'epistemologia moderna e quindi del metodo scientifico; l'approccio euristico è utile ad esempio quando le evidenze da analizzare non trovano precise e complete spiegazioni nella letteratura ufficiale ed è quindi necessario approcciare empiricamente seguendo più percorsi, anche intuitivamente, al fine di generare nuova conoscenza. Il ragionamento inferenziale, nel caso dell'euristica, include il metodo *abduttivo* con il quale è possibile raccogliere il frutto di una analisi iniziale e concentrarlo in una deduzione (o ipotesi investigativa), cioè una affermazione privata la cui validità non è ancora scientifica perché deve essere dimostrata, ad esempio con ragionati e successivi esperimenti di laboratorio. In sostanza, una qualsiasi congettura deduttiva non dimostrata rimane scienza privata, ed è vietata .

*Le credenze antiscientifiche sono nemiche della Giustizia.*

**DEDUZIONE**

Con la deduzione dalla regola generale è possibile prevedere un risultato partendo da un caso specifico:

Regola="i numeri pari sono divisibili per 2 in modo intero"; Caso

in esame="4 è un numero pari".

Risultato predittivo o risposta al quesito: "4 è divisibile per due in modo intero".

**INDUZIONE**

Con la deduzione dalla regola generale è possibile prevedere una regola generale partendo da una successione di Casi: "2 è pari, 2+2 è pari, 2+2+2 è ancora pari".

Risultato predittivo: "10 è pari";

Regola:"un numero pari si può ottenere aggiungendo a 2 n volte 2 con n numero intero".

Oppure

Devo valutare una evidenza (ho trovato il messaggio M sospetto, nello smartphone S). Effettuo dei laboratori su tutti gli smartphone del tipo S, nuovi ed usati e riscontro che tutti quanti generano il messaggio M). Consulto la documentazione ufficiale e formulo la regola del tipo "*tutti gi smartphone del tipo S, in qualsiasi condizione di utilizzo generano il Messaggio M*". Il risultato predittivo sarà: Il messaggio M (sospetto) trovato nello smartphone S non può essere attribuito all'indagato in quanto viene generato in modo automatico in ogni dispositivo di quel tipo.

**ABDUZIONE**

- Lo scienziato Peirce sosteneva che senza *abduzione* non si può fare alcun passo avanti nella scienza. L'abduzione è utile per ipotizzare somiglianze:

- ✦ con ciò che ci aspettiamo sia somigliante
- ✦ con ciò che non ci aspetteremmo sia somigliante
- ✦ con ciò che ancora non conosciamo

Le tre forme di inferenza

| DEDUZIONE | INDUZIONE | ABDUZIONE |
|---|---|---|
| Regola | Caso | Risultato |
| Caso | Risultato | Regola |
| Risultato | Regola | Caso |

- Attenzione: i metodi deduttivo, induttivo e abduttivo possono essere applicati a dati validi ovvero artefatti, con risultati opposti nella risposta al quesito peritale. Per questa ragione non basta che un file esista e sia stato acquisito in modalità di copia forense: è necessario che tale file, prima di essere valutato rispetto al quesito peritale sia categorizzato tramite una *verifica ontologica* per riscontrarne eventuali artefazioni o falsificazioni
  REPERTO❼COPIA FORENSE❼FILE❼**VALIDAZIONE ONTOLOGICA**❼ANALISI
  La verifica ontologica è tuttavia molto laboriosa e dovrebbe essere limitata ai files più importanti.
- La *statistica* viene usata nel perfezionare la lettura dei dati, ad esempio nella ricerca di *indici di frequenza* o di *correlazione* tra vari set di dati.
- La *statistica inferenziale* si esprime nella applicazione di tecniche predittive ad esempio il *test delle ipotesi o della ipotesi nulla* il quale è di grande aiuto per produrre osservazioni di valore scientifico.
- Le prove di *laboratorio* vengono aggiunte laddove necessarie, ad esempio per verificare una ipotesi.
- Gli strumenti usati nei laboratori dovrebbero essere testati su dati di prova. I risultati di ricerche automatiche o calcoli predittivi devono essere supervisionati per la individuazione dei falsi positivi o falsi negativi

## STRUMENTI

Per la consulenza tecnica sono stati usati i seguenti strumenti:

- Windows 10 Professional
- Strumenti di Sistema e Windows Powershell
- FTK IMAGER
- Google Chrome
- Letteratura ufficiale
- Webmail PEC di ARUBA.IT

*_*

## CATENA DI CUSTODIA

La **catena di custodia** dei reperti è stata rispettata a partire dal giorno del prelievo del reperto sino al momento della sua restituzione. La protezione è stata rafforzata utilizzando la cassaforte ignifuga

del CTP: i media digitali sono stati prelevati dal luogo di deposito sicuro solo per poter eseguire le operazioni peritali.

L'ambiente che ospita la cassaforte ed i computer usati nella consulenza è video sorvegliato da un impianto di ultima generazione, di alta qualità costruttiva, collegato 24h/24h con notifiche realtime via smartphone. La riproduzione dei codici Hash nella relazione tecnica (già presenti nel MEDIA allegato alla relazione tecnica) sigilla la catena di custodia con un robusto e semplice criterio di verifica della originalità dei dati.

## ACCESSO A WEB MAIL ARUBA PEC

ACCESSO ALLA CASELLA PEC DEL DOTT. X (COPERTO DA PRIVACY) *-*



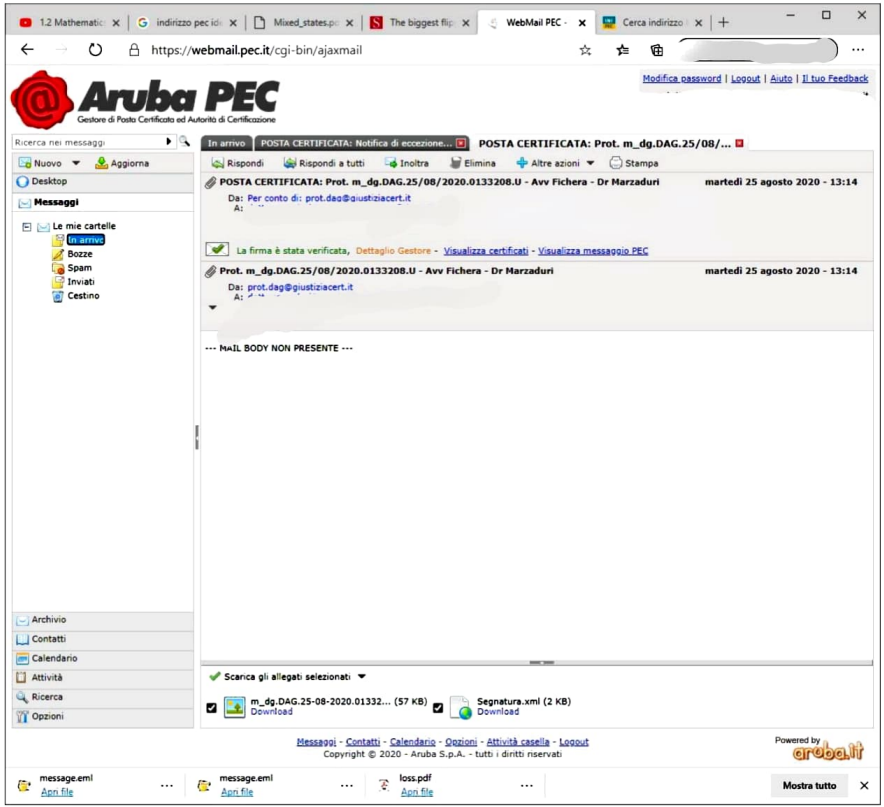
PAGINA DI ACCESSO (9 SETTEMBRE 2020)

ELENCO DEI MESSAGGI PEC RICEVUTI IN ORDINE CRONOLOGICO DISCENDENTE

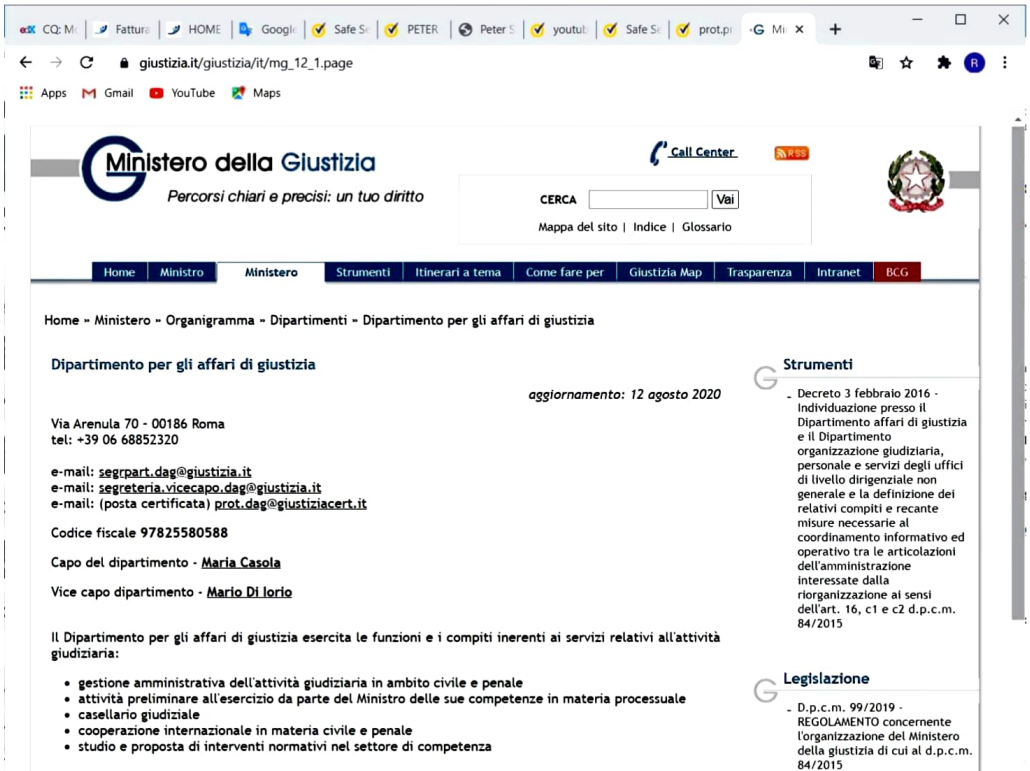
PEC SOSPETTA

*-*

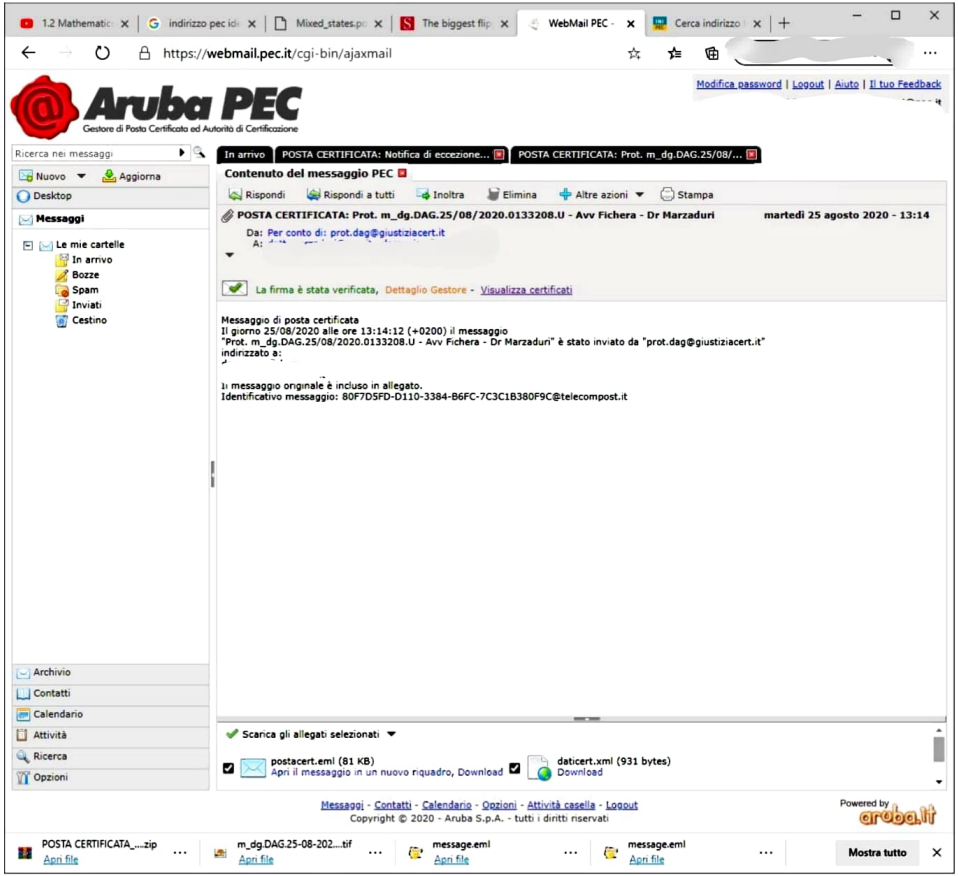
INGRANDIMENTO




PEC SOSPETTA CON ALEGATI POTENZIALMENTE PERICOLOSI*-*




VERIFICA INDIRIZZO DEL MITTENTE INDICATO NELLA PEC SOSPETTA: L'INDIRIZZO ESISTE E FA RIFERIMENTO AD UN UFFICIO DEL MINISTERO DELLA GIUSTIZIA.




PEC SOSPETTA: CONTIENE ALLEGATI.

ALLEGATO FILE m_dg.DAG.25-08-2020.0133208.U.tif



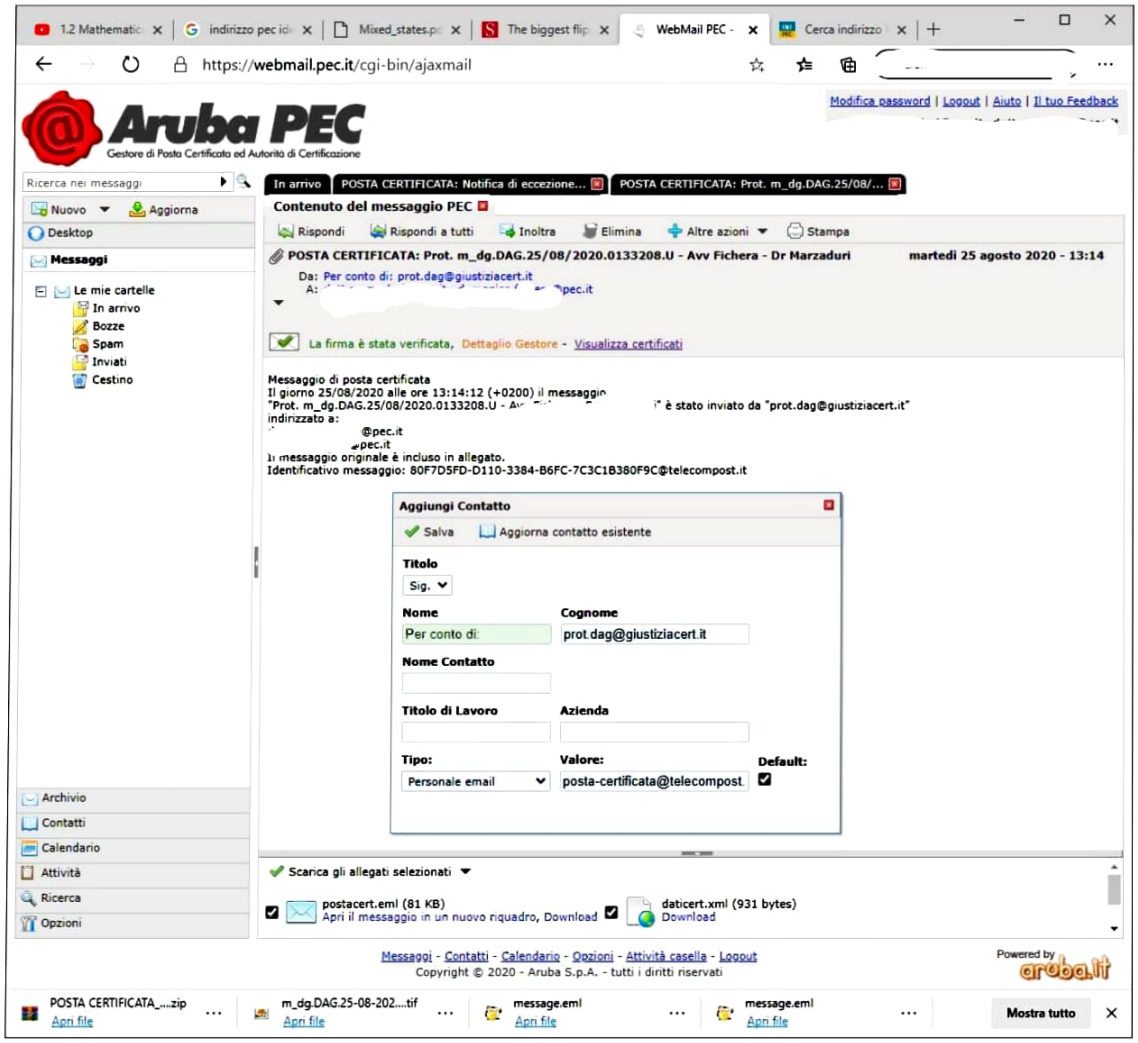
# ANALISI DELL'INDIRIZZO MITTENTE

L'accesso agli attributi estesi del Contatto PEC ha permesso di riscontrare una tecnica di falsificazione dell'indirizzo visualizzato (display address) del mittente della PEC


Risulta infatti che la PEC in questione NON è stata spedita dal dominio GiustiziaCert.it.

Grazie all'uso di tecniche informatiche basata sulla conoscenza specifica degli attributi del directory service della PEC di ARUBA, lo sconosciuto autore della PEC, usando come mittente posta-certificata@telecompost.it ha nascosto il proprio indirizzo dietro l'indirizzo ufficiale prot.dat@giustiziacert.it, quest'ultimo specificato solo come display address.

L'indirizzo PEC è stato ingannevolmente prot.dat@giustiziacert.it simulato utilizzando il campo Cognome.


1.2 Mathematic
indirizzo pec id
Mixed_states.p
The biggest flip
WebMail PEC -
Cerca indirizzo
https://webmail.pec.it/cgi-bin/ajaxmail
Aruba PEC
Gestore di Posta Certificata ed Autorità di Certificazione
Modifica password | Logout | Aiuto | Il tuo Feedback
Ricerca nei messaggi
Nuovo
Aggiorna
Desktop
Messaggi
Le mie cartelle
In arrivo
Bozze
Spam
Inviati
Cestino
Archivio
Contatti
Calendario
Attività
Ricerca
Opzioni
In arrivo
POSTA CERTIFICATA: Notifica di eccezione...
POSTA CERTIFICATA: Prot. m_dg.DAG.25/08/...
Contenuto del messaggio PEC
Rispondi
Rispondi a tutti
Inoltra
Elimina
Altre azioni
Stampa
POSTA CERTIFICATA: Prot. m_dg.DAG.25/08/2020.0133208.U - Avv Fichera - Dr Marzaduri
martedì 25 agosto 2020 - 13:14
Da: Per conto di: prot.dag@giustiziacert.it
La firma è stata verificata, Dettaglio Gestore - Visualizza certificati
Messaggio di posta certificata
Il giorno 25/08/2020 alle ore 13:14:12 (+0200) il messaggio
"Prot. m_dg.DAG.25/08/2020.0133208.U - Avv
" è stato inviato da "prot.dag@giustiziacert.it"
indirizzato a:
@pec.it
pec.it
Il messaggio originale è incluso in allegato.
Identificativo messaggio: 80F7D5FD-D110-3384-B6FC-7C3C1B380F9C@telecompost.it
Aggiungi Contatto
Salva
Aggiorna contatto esistente
Titolo
Sig.
Nome
Per conto di:
Cognome
prot.dag@giustiziacert.it
Nome Contatto
Titolo di Lavoro
Azienda
Tipo:
Personale email
Valore:
posta-certificata@telecompost.
Default:
Scarica gli allegati selezionati
postacert.eml (81 KB)
Apri il messaggio in un nuovo riquadro, Download
daticert.xml (931 bytes)
Download
Messaggi - Contatti - Calendario - Opzioni - Attività casella - Logout
Copyright © 2020 - Aruba S.p.A. - tutti i diritti riservati
Powered by aruba.it
POSTA CERTIFICATA_....zip
Apri file
m_dg.DAG.25-08-202....tif
Apri file
message.eml
Apri file
message.eml
Apri file
Mostra tutto


La falsificazione del mittente è stata eseguita sfruttando i campi del contatto con efficace ed astuta abilità tecnica.

Il ricevente Dott. (Coperto da Privacy) è stato tratto in inganno dall'indirizzo PROT.DAG@GIUSTIZIACERT.IT che corrisponde effettivamente alla PEC di un ufficio giudiziario.

# **PARTE SECONDA** COPIA IMMAGINE E VALIDAZIONE FORENSE

---

Il CTP si è attenuto alle indicazioni generali vigenti in merito alla produzione delle copie forensi declinandole al caso di fattispecie.

**Sono state eseguite le copie forensi dei messaggi PEC acquisiti.**

Per la produzione delle *copie forensi* sono stati soddisfatti i seguenti requisiti tecnici e procedurali:

- L'operatore che produce la copia forense deve essere qualificato professionalmente e deve operare in modo tale da minimizzare i rischi di perdita irreversibile dei dati contenuti nei reperti.
- La strumentazione deve essere testata da istituti specializzati e riconosciuti dalla comunità scientifica forense, ad esempio il NIST, National Institute of Standards and Technology.

- Gli strumenti scelti vanno utilizzati secondo le indicazioni dei produttori. È preferibile eseguire una prova per verificarne le funzionalità e gli eventuali falsi positivi.
- Per le memorie digitali come hard disk è bene verificare l'effettivo blocco in scrittura della porta fisica di collegamento.
- È necessario creare una immagine della memoria o del file da acquisire.
- Lo strumento informatico usato per la duplicazione (copia immagine o Mirror) non deve alterare il dispositivo che contiene i dati da acquisire. Quando ciò non fosse possibile la modifica del reperto, ad esempio la inoculazione di un agente software di estrazione dei dati, deve essere nota e non deve interessare i dati che saranno usati come prove.
- Lo strumento informatico deve essere in grado di verificare l'integrità di un'immagine digitale e di autenticare la copia come corrispondente con l'originale. A questo scopo viene in aiuto la matematica dei numeri primi e gli algoritmi di Hashing. Gli algoritmi Hash devono essere noti e verificabili (per maggiori approfondimenti si consulti il sito del NSA  National Security Agency.

- Lo strumento informatico usato per le copie immagine deve registrare in un file gli eventuali errori di accesso in lettura e scrittura.
- Deve essere possibile sapere se la copia immagine è completa ovvero parziale poiché limitata da condizioni ostative. Nel caso in cui la estrazione fosse stata parziale sarà compito del Consulente tentare l'estrazione dei dati rimanenti integrando anche altre tecniche.
- I dati clonati/copiati/estratti devono essere associati ai codici univoci come SHA1. Ripetendo il calcolo degli Hash sulla copia forense si potrà riscontrare in qualsiasi momento futuro l'uguaglianza ovvero l'eventuale differenza rispetto ai codici Hash originali della copia forense.
- L'estrazione dei dati in modalità forense può essere limitata (per ragioni di privacy o copyright) alla porzione di interesse per la indagine. Tale porzione deve essere tuttavia completa e non nascondere elementi correlabili con i dati di interesse necessari alla loro identificazione e descrizione, validazione ontologica, validazione forense o di complemento.
- Il Consulente Tecnico potrà autenticare la copia immagine come **copia forense** solo dopo aver verificato positivamente:
    - la strumentazione e le condizioni iniziali d'uso, o la copia immagine, i relativi file di log ed i codici univoci Hash,
- Deve essere preservata la catena di custodia e mantenuta la massima riservatezza dei dati acquisiti così come dei reperti da cui i dati sono stati acquisiti.

*_*

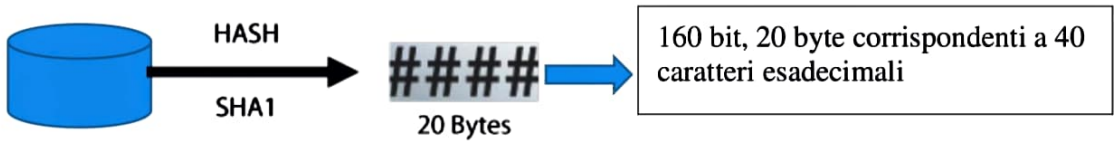
*NOTA TECNICA Le funzioni Hash possono essere generate da funzioni di compressione, cioè da funzioni*
*lunghezza fissata ma inferiore.*

*Un codice Hash di una immagine digitale (di un disco o file) è, da un punto di vista computazionale, una b*
*caratteristica di essere unica: la funzione Hash SHA-1 scelta in questa consulenza tecnica è una funzione*
*possono esistere (esistenza in termini computazionali) due differenti immagini digitali (copie) con lo stess*

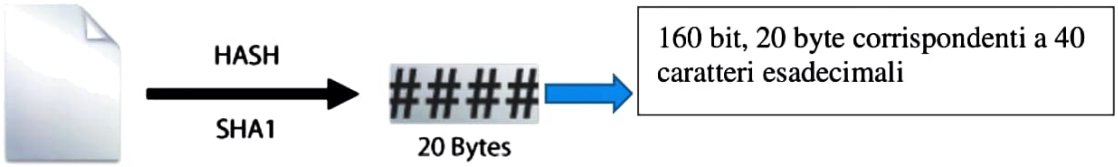
*La funzione Hash SHA-1 scelta in questa consulenza tecnica è una funzione resistente alle contro immagin*
*esso deriva.*

*Una impronta digitale Hash è una rappresentazione alfanumerica, sintetica ed unica di un file o uno strea*
*codici Hash, è fondamentale nella scienza forense informatica.*

*Maggiori informazioni sugli algoritmi SHA pubblicati dalla NSA organismo della sicurezza degli USA son*




*Hard disk*




*Copia immagine*

*FIGURA: quando il media fisico e la sua copia immagine hanno la medesima impronta digitale HASH cal*
*identiche e possono essere validate dal CT come copie forensi.*

*-*

*Una panoramica autorevole del processo di imaging di un disco è disponibile ad esempio presso il NIST's Disk Imaging Tool Specification (Version 3.1.6).*

## STRUMENTI SOFTWARE

Per la produzione delle *copie forensi*, il CTP ha scelto

- FTKIMAGER

Tutto il software forense è stato usato dal CT nel totale rispetto legale di ciascuna licenza d'uso senza alterare i dati utente.

*-*

# VALIDAZIONE FORENSE DELLE COPIE IMMAGINE

**La validazione delle copie immagine è un compito del CT e non dello strumento.**

La procedura di validazione è stata eseguita calcolando i codici HASH e riportando le impronte SHA1 in questa relazione.

Per le *impronte digitali Hash* dei file sono stati usati algoritmi della famiglia SHA (128, 256, 512bit, e superiori). Le funzioni Hash hanno una caratteristica speciale che le rendono usabili nella scienza forense: non esiste la possibilità che due differenti file (cioè file con differente contenuto) possano generare la medesima impronta Hash. Con i codici Hash è possibile identificare univocamente ogni file o intero disco con un codice alfanumerico molto sintetico (di qualche decina di caratteri), di facile rappresentazione. Inoltre, l'utilizzo dei codici Hash permette anche di verificare nel tempo la alterazione dei file: ricalcolando il codice Hash di un file o di un disco sarà possibile verificare se corrisponde con l'originale riportato nella perizia forense e nel caso di uguaglianza si potrà stare tranquilli: il file è uguale all'originale estratto dal dispositivo fisico.

La computazione del codice Hash di un file non tiene mai conto del nome del file ma solo del suo contenuto ovvero il codice Hash di un disco certifica contenuto e proprietà di ogni singolo file.

-**

NOTA. Si segnala che i percorsi (pathname) indicati nei log si riferiscono al dispositivo forense di creazione.

**FILES ACQUISITI E CODICE HASH SHA1**

```
Created By AccessData® FTK® Imager 4.3.0.18


Case Information:
Acquired using: ADI4.3.0.18
Case Number: PERIZIA PEC DOTT. (COPERTO DA PRIVACY)-SETTEMBRE
2020
Evidence Number: R1
Unique Description: CARTELLA FILES CON PEC SOSPETTA E NOTIFICHE



------------------------------------------------------------
```

```
Information for
D:\MYSTORE\DATI\Alice\2020\FORENSICS\CTP\(COPERTO DA
PRIVACY)\PEC MALWARE\R1.ad1:

[Computed Hashes]
 MD5 checksum:    a62b369be9738e6900b83414a0cf1454
 SHA1 checksum:   58e7ac98cb724c12749b37f084de0978abcdda89

Image information:
 Acquisition started:   Thu Sep 10 10:48:58 2020
Acquisition finished:  Thu Sep 10 10:49:00 2020
Segment list:
  D:\MYSTORE\DATI\Alice\2020\FORENSICS\CTP\(COPERTO DA
PRIVACY)\PEC
MALWARE\R1.ad1

Image Verification Results:
 Verification started:  Thu Sep 10 10:49:00 2020
 Verification finished: Thu Sep 10 10:49:00 2020
 MD5 checksum:    a62b369be9738e6900b83414a0cf1454 : verified
 SHA1 checksum:   58e7ac98cb724c12749b37f084de0978abcdda89 :
verified
```

***IL CT, DOPO AVER CALCOLATO E VERIFICATO LE IMPRONTE DIGITALI HASH CERTIFICA LA VALIDITÀ AI FINI FORENSI DEI FILES PRODOTTI CON QUESTA PERIZIA***.

# CONCLUSIONI

Gli accertamenti tecnici in materia di informatica forense sono stati compiuti nel rispetto delle indicazioni contenute nella lettera di incarico peritale, dell' "*Electronic Evidence Guide*" (COE Concilio di Europa), delle "*Linee guida in materia di trattamento di dati personali da parte dei consulenti tecnici e dei periti ausiliari del giudice e del pubblico ministero*", Gazzetta Ufficiale n. 178 del 31 luglio 2008 Registro delle deliberazioni Del. n. 46 del 26 giugno 2008" e della normativa vigente.

Il CTP ha accuratamente raccolto ed analizzato i messaggi della PEC sospetta indicata dal Dott. (COPERTO DA PRIVACY).

Per la copia forense, le ricerche e l'analisi sono stati scelti strumenti software di ultima generazione e con regolare licenza d'uso.

Per la autenticazione digitale sono stati usati algoritmi SHA1 usati nella comunità forense internazionale e riconosciuti dall'European Union Agency for Network and Information Security


La verifica della originalità ed integrità dei dati delle copie forensi potrà essere eseguita in futuro, confrontando i codici Hash riprodotti in questa relazione con i relativi codici ricalcolati sui files.

*-*

Il messaggio PEC sospetto include una falsificazione del mittente, astutamente eseguita sfruttando i campi tecnici del contatto del mittente medesimo, i quali sono usati dalla webmail app solo nella visualizzazione del messaggio. Per questa ragione il reale indirizzo del mittente viene automaticamente nascosto a destinatario che in questo caso è stato tratto in inganno da un indirizzo esistente del Ministero della Giustizia ma falsificato come indirizzo del mittente.

L'operazione, pur non avendo alterato illegalmente il sistema Aruba è il risultati di una efficace ed astuta abilità tecnica dello sconosciuto mittente, il quale ha manipolato i campi del contatto facendo figurare al destinatario, il Dott. (Coperto da Privacy), non il reale indirizzo PEC del mittente ma quello di un ufficio del Ministero della Giustizia.

Il ricevente Dott. (Coperto da Privacy) è stato tratto inevitabilmente tratto in inganno dall'indirizzo PROT.DAG@GIUSTIZIACERT.IT usato come falsificazione del reale indirizzo postacertificata@telecompost.it

Tramite questo inganno il Dott. (Coperto da Privacy) ha creduto inevitabilmente che la PEC fosse stata spedita dal Ministero della Giustizia anziché dallo sconosciuto posta-certificata@telecompost.it *-*

Facendo leva sulla fiducia e timore indotti da una PEC proveniente (falsamente) dal Ministero, lo sconosciuto autore posta-certificata@telecompost.it ha verosimilmente voluto creare un contesto tale da obbligare il Dott. (Coperto da Privacy) ad aprire il messaggio ed il suo allegato con il potenziale ed ulteriore pericolo che tale allegato potesse contenere un virus. In letteratura questa tecnica è nota come social Engineering.

Inoltre, grazie alla falsificazione, è quasi certo (o altamente probabile) che il mittente volesse attribuire originalità ed ufficialità al contenuto della PEC falsificata, inducendo di conseguenza il Dott. (Coperto da Privacy) ad intraprendere iniziative legali o altre azioni non necessarie e forse controproducenti, poiché basate su un falso.