COMPUTER FORENSICS

Lezione 23: Fase Finale
la Relazione Tecnica

SICUREZZA SISTEMI RETI INFORMATICHE

UNIVERSITA' DEGLI STUDI DI NAPOLI FEDERICO II

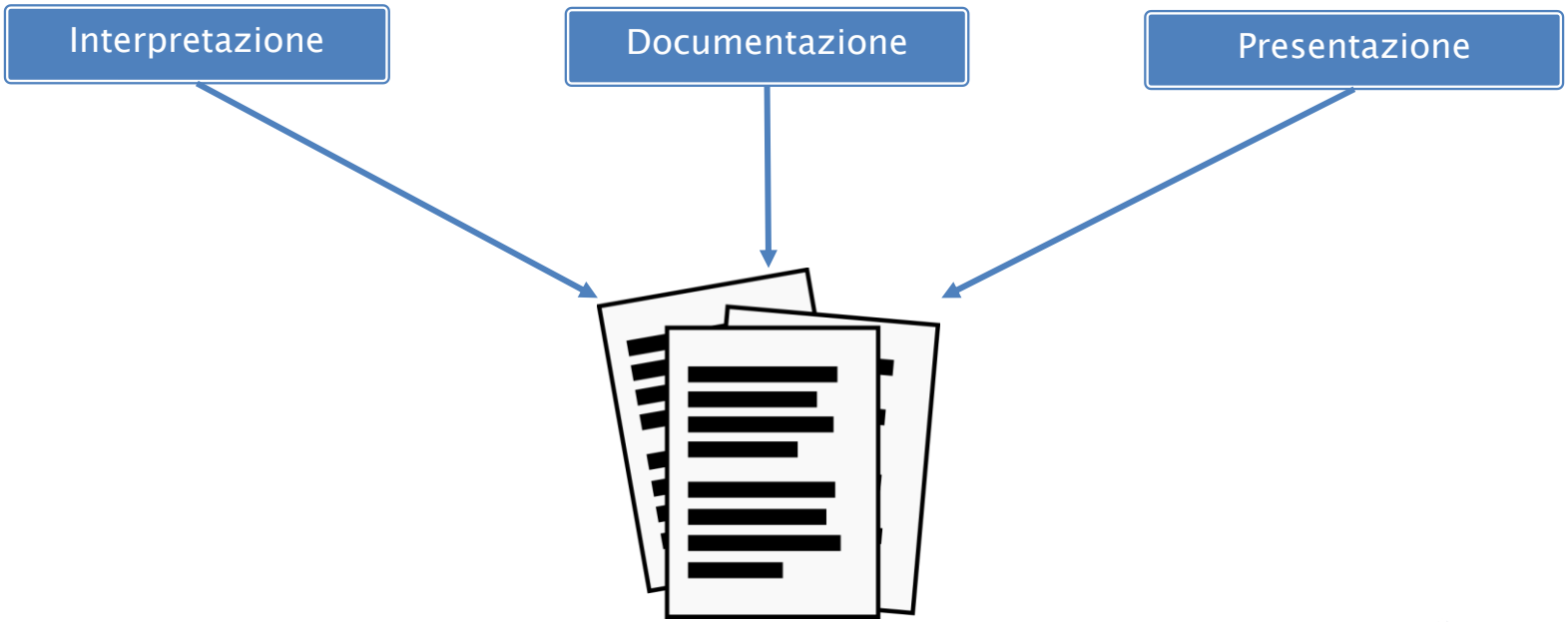
A.A. 2021/22

Dott. Lorenzo LAURATO

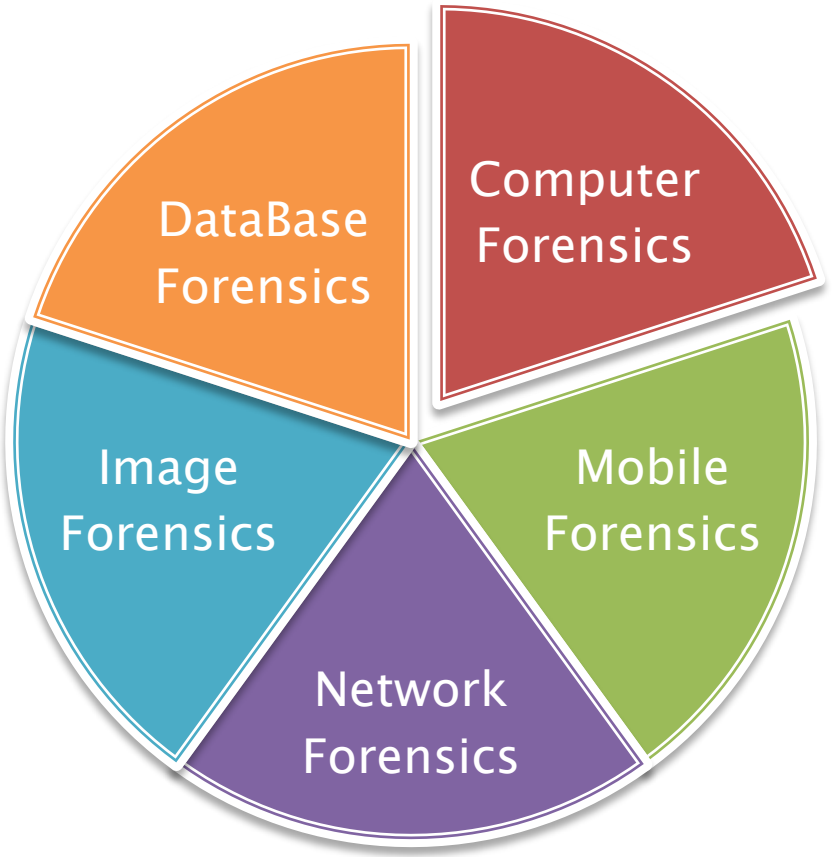
Fasi

- Identificazione
- Raccolta
- Validazione
- Preservazione
- Analisi
- **Interpretazione**
- **Documentazione**
- **Presentazione**

Fasi


Interpretazione
Documentazione
Presentazione
Relazione Tecnica

Digital Forensics



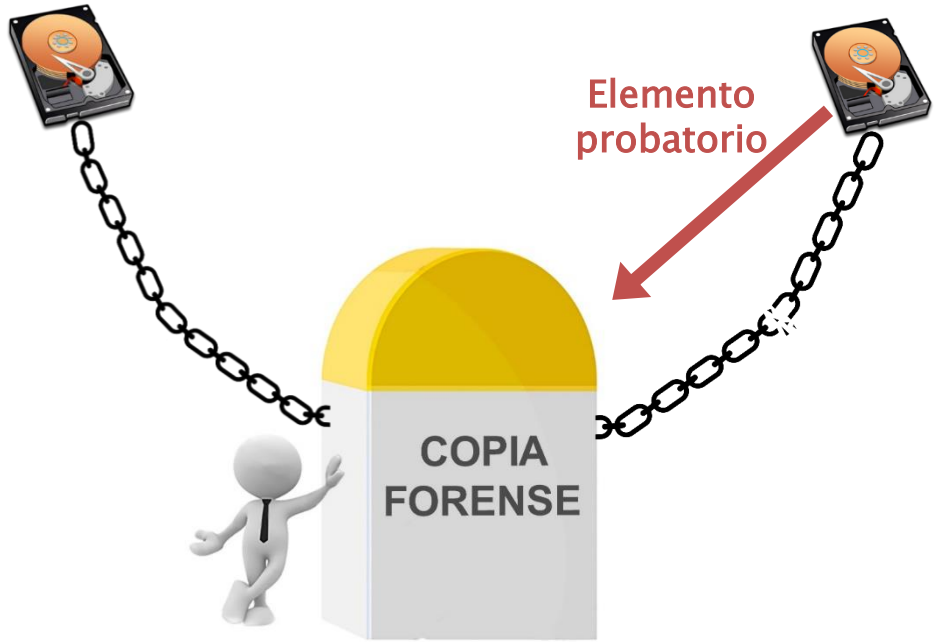
La prova digitale

- CONTRO:
  - Facilmente corruttibile
- PRO:
  - Duplicazione

Accertamenti…

Accertamento tecnico ripetibile

Accertamento tecnico irripetibile



Accertamento tecnico ripetibile

L'accertamento ripetibile

- Agire in modo da non alterare la prova
- **Agire in modo da documentare ogni azione compiuta su di essa**
- **Porre la controparte in condizione di replicare quanto fatto**

La relazione tecnica

- Base di partenza: quesito
- Descrizione degli strumenti Hardware e Software impiegati
- Descrizione delle azioni che hanno portato/non portato risultati
- **Scopo**: chiunque deve poter giungere alle medesime conclusioni

La relazione tecnica

ESEMPIO: *indagine di pedopornografia*

1. Ricerca di immagini residenti
2. Ricerca di immagini in archivi compressi e posta elettronica
3. Ricerca di programmi P2P *(Es.: eDonkey, BitTorrent, etc.)*
   a) Diffusione?
4. Ricerca file cancellati
5. Ricerca di periferiche di archiviazione agganciate
6. Analisi steganografica

La relazione tecnica

- Descrizione dettagliata di hardware e software impiegato

deft

Autopsy®
BASIS TECHNOLOGY

Eric Zimmerman's
TOOLS

ACCESSDATA
ForensicToolkit (FTK)

INTERNET
EVIDENCE
FINDER™

La relazione tecnica

Descrizione e valutazioni

- Parte Descrittiva: dettagliata ed accurata:
  - Documentazione fotografica
- Parte valutativa:
  - Motivazioni
  - Descrizione dell'iter logico
  - *Giuridicamente non è vincolante*

La relazione tecnica

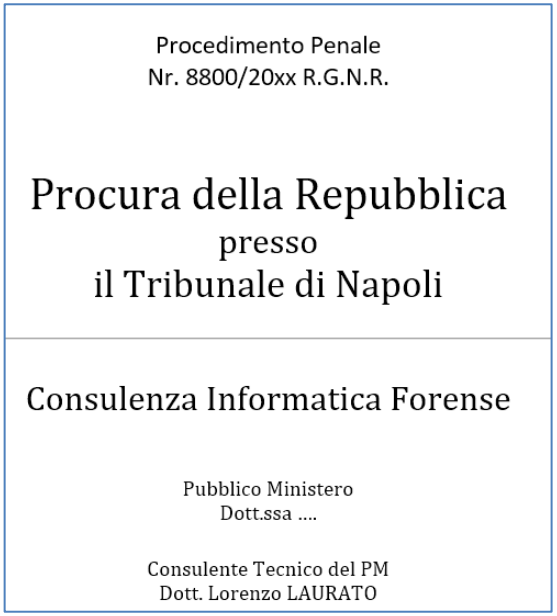
Forma

- Quattro parti:
  - Parte Epigrafica: *indicazione degli estremi del P.P., P.M., Giudice, descrizione dell'incarico, parti presenti ad un accertamento, etc.*
  - Parte Descrittiva: *illustrazione degli accertamenti e/o ricostruzioni compiuti*
  - Parte Valutativa: *risposta ai quesiti con motivazione esaustiva delle conclusioni*
  - Parte Riassuntiva: *esposizione sintetica della risposta ad ogni quesito*
- Chiara ed intellegibile:
  - Impiego di grafici, illustrazioni, tabelle, etc.

La relazione tecnica

Forma

1) Parte Epigrafica: *indicazione degli estremi del P.P., P.M., Giudice, descrizione dell'incarico, parti presenti ad un accertamento, etc.*



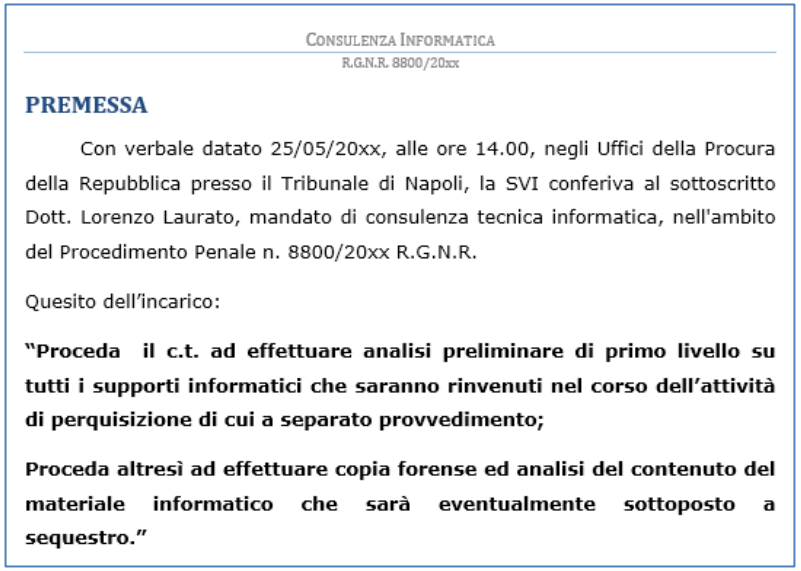
Procedimento Penale
Nr. 8800/20xx R.G.N.R.

Procura della Repubblica
presso
il Tribunale di Napoli

Consulenza Informatica Forense

Pubblico Ministero
Dott.ssa ....

Consulente Tecnico del PM
Dott. Lorenzo LAURATO



CONSULENZA INFORMATICA
R.G.N.R. 8800/20xx

PREMESSA

Con verbale datato 25/05/20xx, alle ore 14.00, negli Uffici della Procura della Repubblica presso il Tribunale di Napoli, la SVI conferiva al sottoscritto Dott. Lorenzo Laurato, mandato di consulenza tecnica informatica, nell'ambito del Procedimento Penale n. 8800/20xx R.G.N.R.

Quesito dell'incarico:

"Proceda il c.t. ad effettuare analisi preliminare di primo livello su tutti i supporti informatici che saranno rinvenuti nel corso dell'attività di perquisizione di cui a separato provvedimento;

Proceda altresì ad effettuare copia forense ed analisi del contenuto del materiale informatico che sarà eventualmente sottoposto a sequestro."

La relazione tecnica

Forma

2) Parte Descrittiva: *illustrazione degli accertamenti e/o ricostruzioni compiuti*

CONSULENZA INFORMATICA
R.G.N.R. 8800/20xx

Le acquisizioni dei supporti di memoria da analizzare vengono effettuate impiegando, a seconda del caso:

- il **"Forensic Quest"** e/o il **"Forensic Dossier"**, prodotti dalla "Logicube" e/o il **"Forensic Duplicator TD1"** della "Tableau", dispositivi hardware autonomi, con sistema operativo Linux based embedded, concepiti per la realizzazione di copie forensi di qualsiasi tipo di hard disk: le modalità di funzionamento degli strumenti impediscono qualsiasi tipo di scrittura, anche accidentale, sul supporto di origine, preservandone il contenuto.

CONSULENZA INFORMATICA
R.G.N.R. 8800/20xx

Tecnica

L'analisi

L'analisi delle immagini prodotte dal dispositivo mobile è stata eseguita impiegando lo strumento della Cellebrite Ltd denominato "**UFED Physical Analyzer 5.1**".

CONSULENZA INFORMATICA
R.G.N.R. 8800/20xx

CELSAM – Cellulare Samsung SM-G357FZ (Galaxy Ace 4) – S.N.:xxx

Il reperto catalogato **"CELSAM"**, relativo al dispositivo Cellulare Samsung SM-G357FZ Galaxy Ace 4, è stato acquisito impiegando lo strumento denominato Cellebrite UFED, così come specificato nei paragrafi iniziali della presente relazione.

Tale acquisizione non ha permesso di estrapolare i dati delle applicazioni presenti sul dispositivo e nella fattispecie, l'applicazione di messaggistica istantanea denominata "WhatsApp".

Per tale motivo solo per l'estrazione dei database dell'applicazione "WhatsApp" è stato impiegato lo strumento software denominato "**WhatsApp Xtract 2.5.8**".

La relazione tecnica

Forma

3) Parte Valutativa: *risposta ai quesiti con motivazione esaustiva delle conclusioni*

Una prima analisi sulla memoria del dispositivo è stata eseguita allo scopo di determinare la presenza del reato di "*stalking*" compiuto ai danni della p.o. "**Maria ROSSI**". Da tale analisi si evidenziano i seguiti riscontri:

La ricerca all'interno della rubrica del dispositivo cellulare in oggetto eseguita mediante il nominativo e l'utenza telofonica della p.o. "Maria ROSSI" ha avuto esito negativo.

Successivamente è stata eseguita una ricerca, mediante l'utenza telefonica della p.o., nell'intero contenuto del dispositivo: ciò ha evidenziato la presenza di nr. 2 elementi all'interno del registro chiamate:

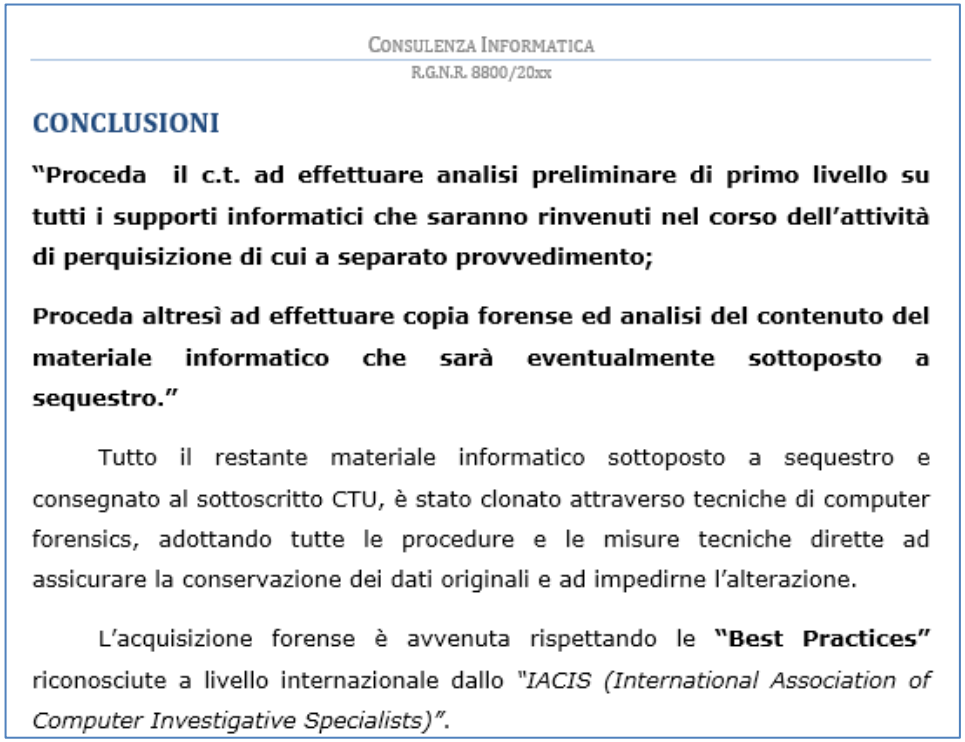
From: +3[redacted]	Scricciolo	22/12/2015 17:24:19(UTC+0)	00:01:10	Incoming
To: +393[redacted]	Scricciolo	22/12/2015 17:23:40(UTC+0)	00:00:00	Outgoing

Da tale evidenzia inoltre si può presumere che precedentemente l'utenza telefonica della p.o. era rubricata all'interno del dispositivo cellulare con il nominativo "**Scricciolo**".

La relazione tecnica

Forma

4) Parte Riassuntiva: *esposizione sintetica della risposta ad ogni quesito*



CONSULENZA INFORMATICA

R.G.N.R. 8800/20xx

CONCLUSIONI

"Proceda il c.t. ad effettuare analisi preliminare di primo livello su tutti i supporti informatici che saranno rinvenuti nel corso dell'attività di perquisizione di cui a separato provvedimento;

Proceda altresì ad effettuare copia forense ed analisi del contenuto del materiale informatico che sarà eventualmente sottoposto a sequestro."

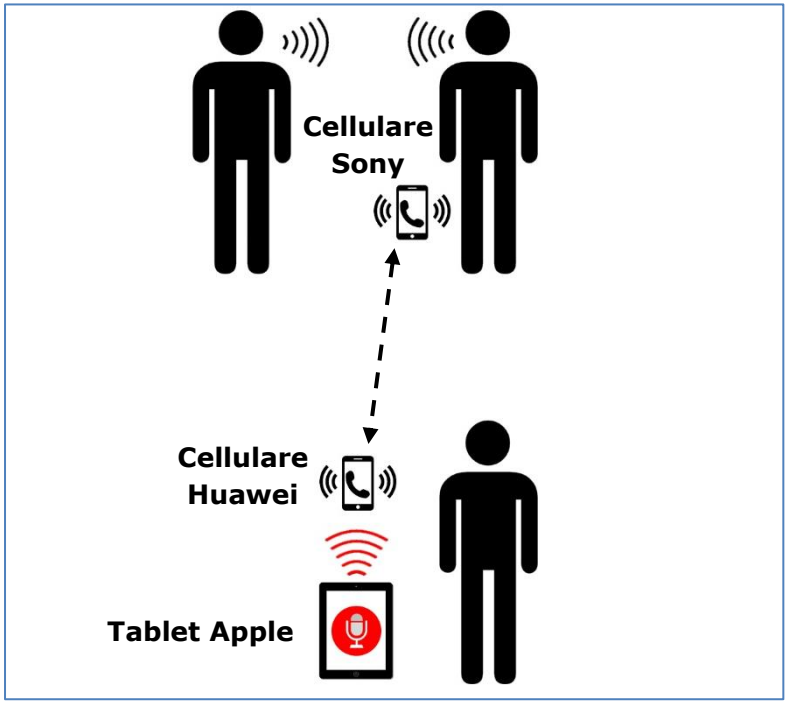
Tutto il restante materiale informatico sottoposto a sequestro e consegnato al sottoscritto CTU, è stato clonato attraverso tecniche di computer forensics, adottando tutte le procedure e le misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione.

L'acquisizione forense è avvenuta rispettando le **"Best Practices"** riconosciute a livello internazionale dallo *"IACIS (International Association of Computer Investigative Specialists)"*.

La relazione tecnica

Forma

- Chiara ed intellegibile:
  - Impiego di grafici, illustrazioni, tabelle, etc.



Digital Forensics

- Un caso di Computer Forensics

SSRI
Sicurezza Sistemi Reti Informatiche

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II

a.a. 2021/22