Università degli Studi di Catania

-----BEGIN PGP MESSAGE-----
Version: PGP 7.1

qANQR1DDDQQDAwLnVMzaiSSEk2D
JTCm8GgOeA6a6Rq4dWGAHRIPgYxrF
R7/b0lFa
1p5yz/
WAVN42KyCV6QLFsyWTTGgvH9p1th
8gXHz7aLLC3aYyXFldhHu6bvaDEbQc
d94=
=VqZj
-----END PGP MESSAGE-----

COMPUTER FORENSICS
CORSO DI LAUREA IN INFORMATICA

Le tecnologie per il trattamento dei reperti informatici

A.A. 2010/2011

Dott. Donato Eugenio Caccavella

Un approccio metodologico

Il dato informatico, questo sconosciuto

È una successione di bit, cioè di 0 e di 1, registrati all'interno di un dispositivo.

Il dato informatico, questo sconosciuto

Esempio:

Ciao = 00101001010001011110101010101010

Il dato informatico, questo sconosciuto

E' esistito almeno un momento in cui tali bit erano registrati su un dispositivo il cui stato, impartendo opportuni comandi, poteva essere modificato da un operatore.

Il dato informatico, questo sconosciuto

Non è possibile accertare eventuali modifiche apportate in precedenza a singoli bit

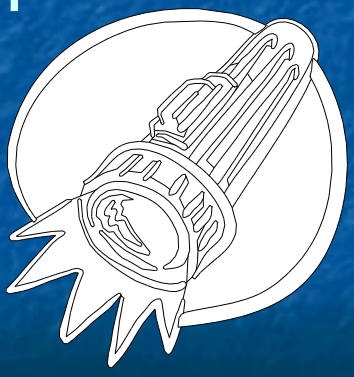
Il dato informatico, questo sconosciuto…

Allora il dato è inattendibile ?

No !
Un esempio ?
la Firma Digitale

Il dato informatico, questo sconosciuto…

Esempio di bit:



De reperto informatico

Tenendo ben presente la **volatilità del dato informatico** esaminiamo il reperto informatico

De reperto informatico

5 fasi trattamento:

- individuazione
- acquisizione
- analisi
- valutazione
- presentazione

Individuazione
del reperto informatico:

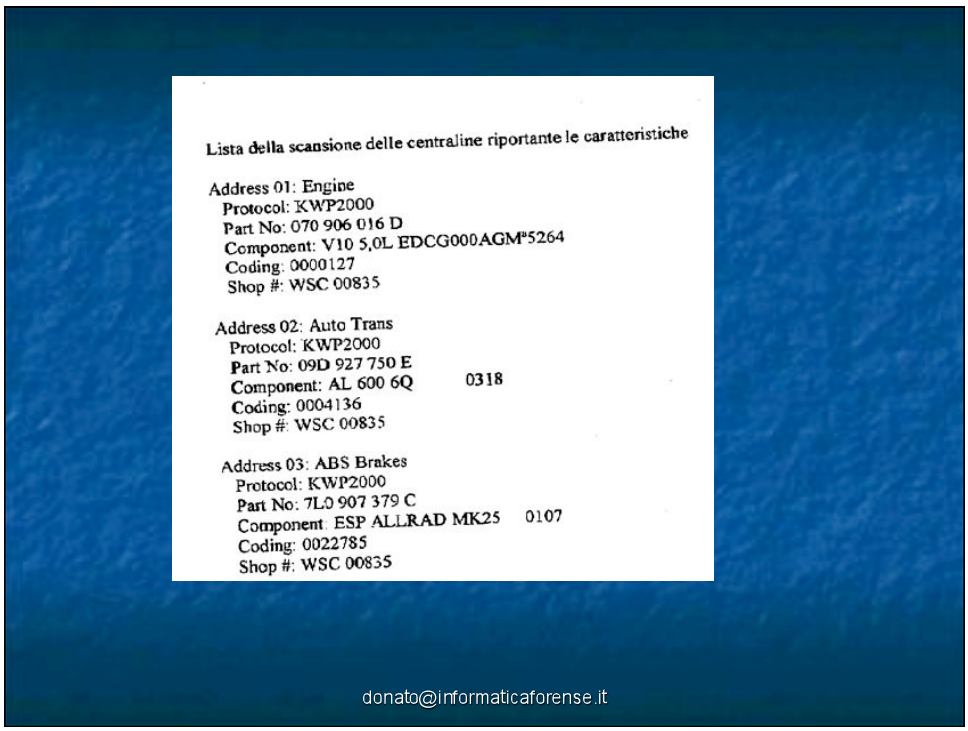
deve essere esaustiva!

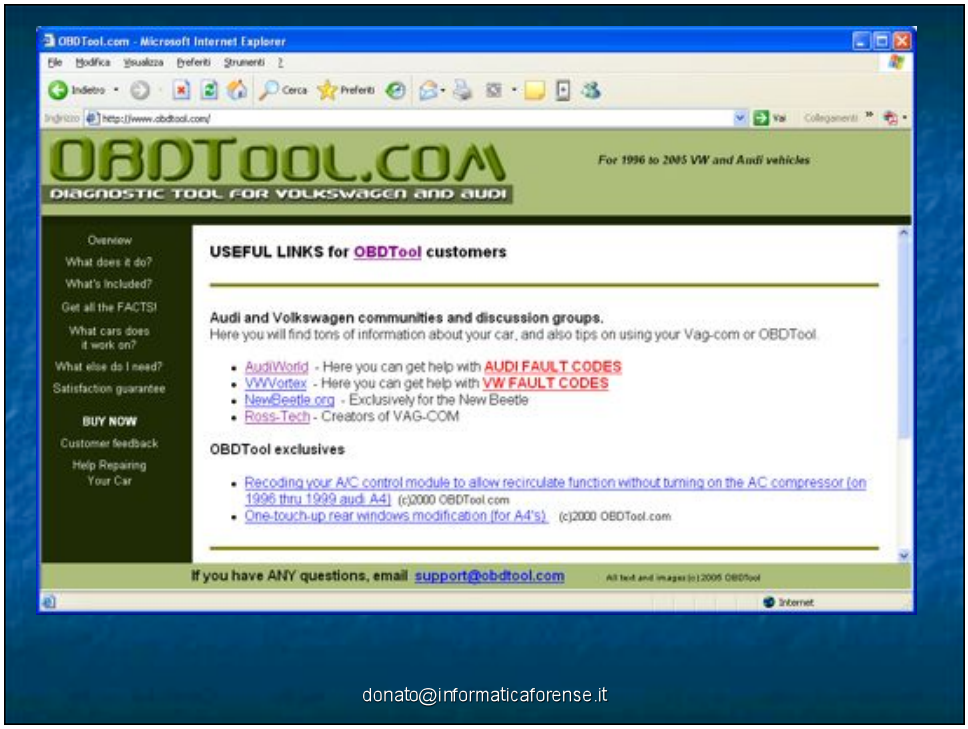
Vanno individuati tutti i dispositivi che possono contenere dati digitali o digitalizzati:

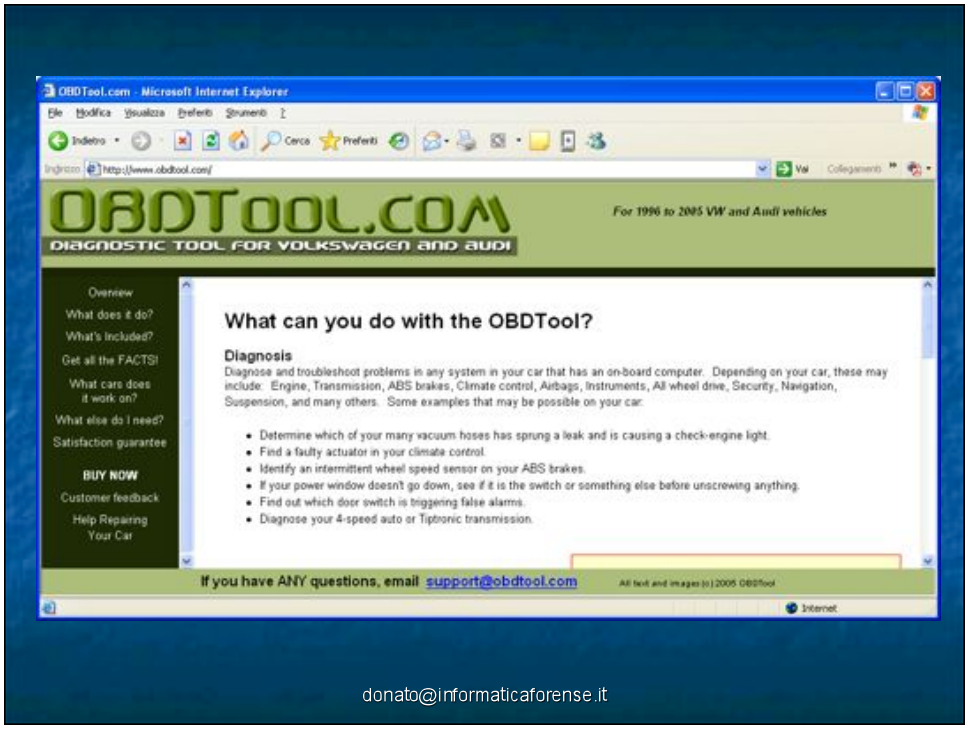
Es. Video camere, cellulari, automobili, agende elettroniche, elettrodomestici, fax, fotocopiatori, etc.

A proposito di individuazione….


STOP
GUASTO TELAIO:
RECARSI
P
R
N
D
S
442.4 km
3:47
65852 km
donato@informaticaforense.it


Lista della scansione delle centraline riportante le caratteristiche
Address 01: Engine
Protocol: KWP2000
Part No: 070 906 016 D
Component: V10 5,0L EDCG000AGM 5264
Coding: 0000127
Shop #: WSC 00835
Address 02: Auto Trans
Protocol: KWP2000
Part No: 09D 927 750 E
Component: AL 600 6Q 0318
Coding: 0004136
Shop #: WSC 00835
Address 03: ABS Brakes
Protocol: KWP2000
Part No: 7L0 907 379 C
Component: ESP ALLRAD MK25 0107
Coding: 0022785
Shop #: WSC 00835
donato@informaticaforense.it





donato@informaticaforense.it

donato@informaticaforense.it

Individuazione & marketing
Il datawarehouse…

Soluzione software in base al quale i dati sono estratti da ampi data base relazionali e altre sorgenti e memorizzati in data base minori tra loro collegati per rendere più agevoli le analisi. I responsabili dei nuovi business possono accedervi per estrarre le informazioni di "conoscenza" e consentire le analisi sui processi e le opportunità

www.datacontact.it

Individuazione & marketing

Il datawarehouse…

Accezione forense:

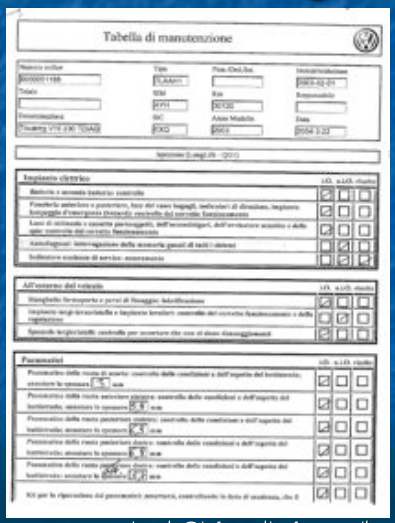
Insieme di dati con elevato valore indiziario

di ampia visibilità facilmente interrogabili..

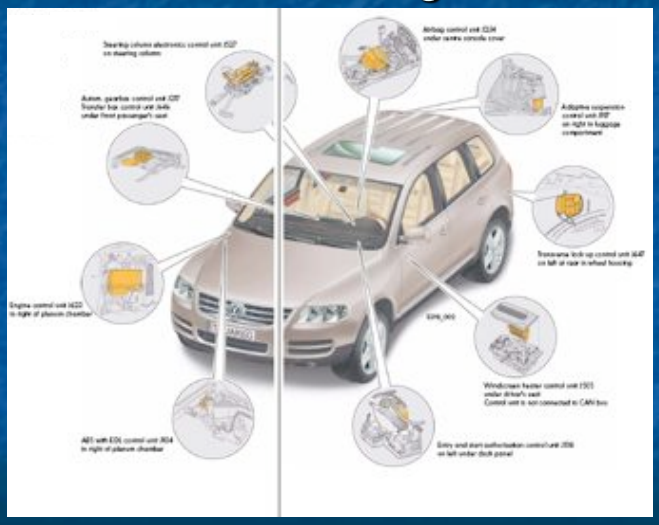
Es. Un gestore di telefonia… lo vediamo dopo

La certificazione di qualità…

…le conseguenze!

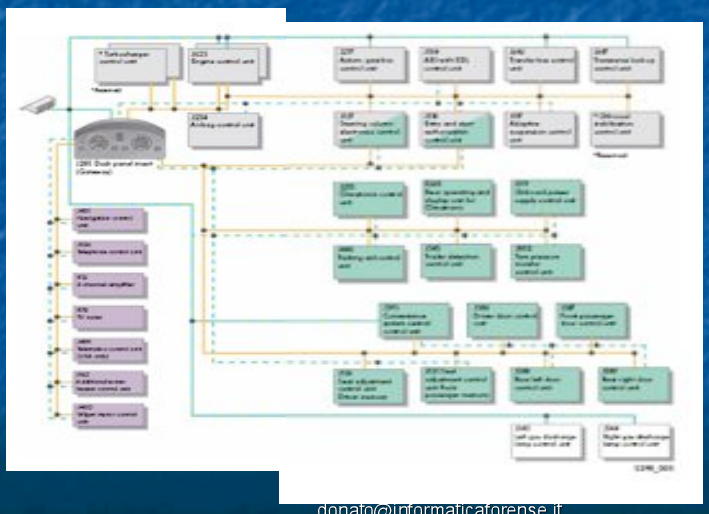


Elenco centraline elettroniche presenti nel Volkswagen Touareg

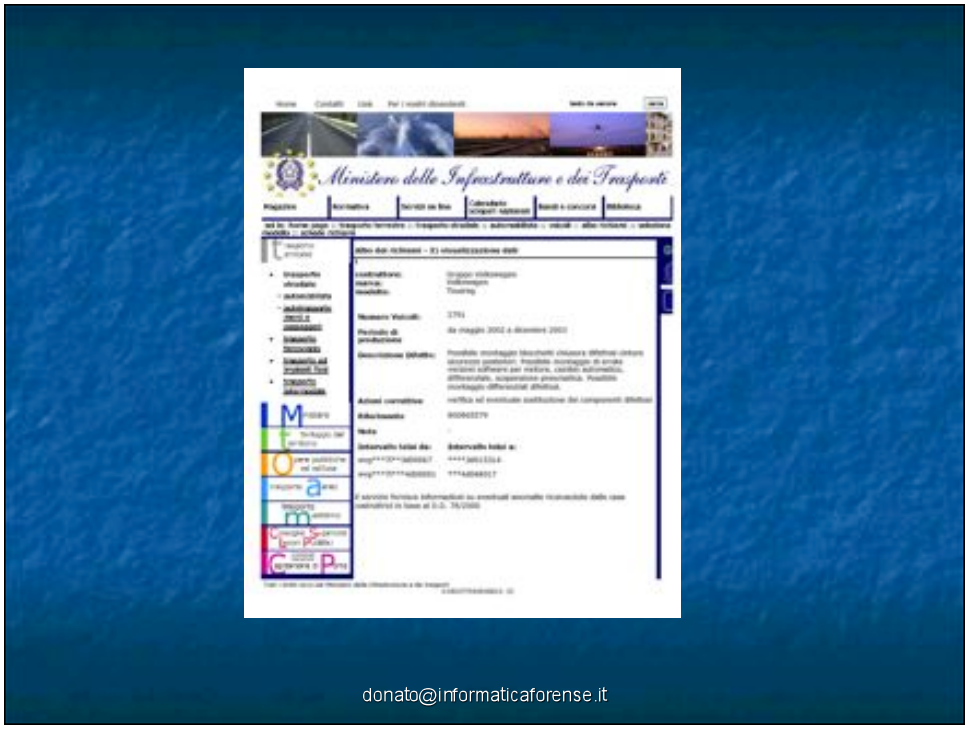


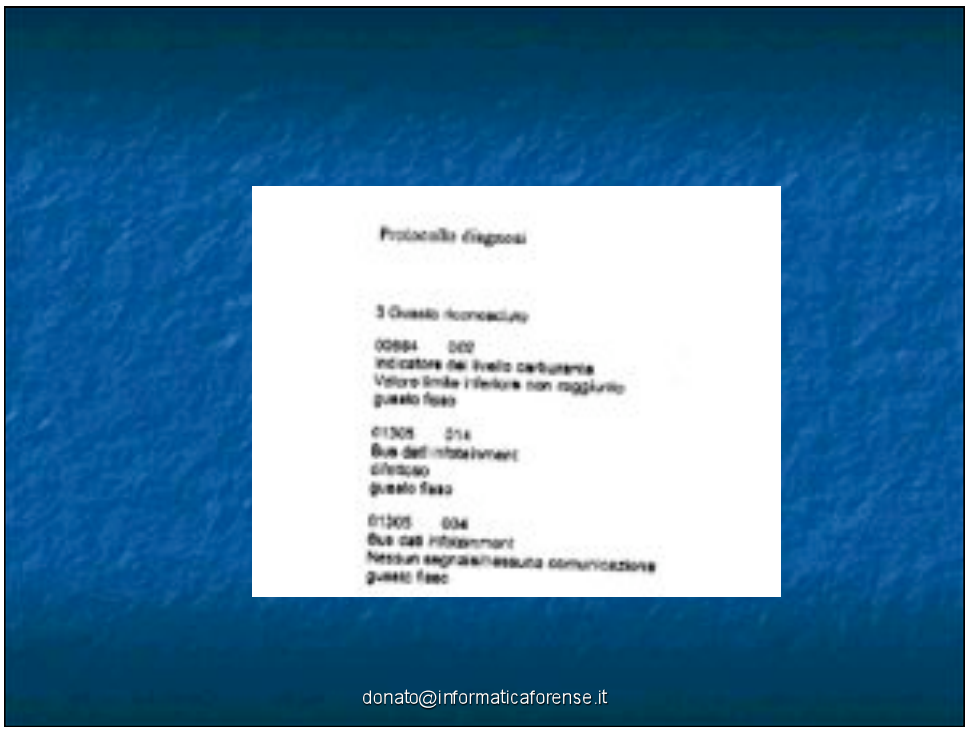
donato@informaticaforense.it

Elenco centraline elettroniche presenti nel Volkswagen Touareg



donato@informaticaforense.it


Ministero delle Infrastrutture e dei Trasporti
donato@informaticaforense.it


Protocollo diagnosi
donato@informaticaforense.it

Conclusioni

"il veicolo mostra un guasto fisso sulla componete del "BUS DATI"e tale guasto implica funzionamenti anomali ed imprevedibili del veicolo anche durante la marcia, rendendolo di conseguenza inidoneo alla marcia su strada"

donato@informaticaforense.it

Acquisizione del reperto informatico:

deve essere completa!

Mentre accade di vedere nei Tribunali che la PG acquisisca:
- la stampa delle proprietà del documento di MSWord anziché il reperto stesso;

- fax composto di tre frammenti delle istruzioni di un programma che a detta del PM è un "demone"

Acquisizione del reperto informatico:

deve essere accurata!

Non è necessario acquisire l'intero Personal Computer, ma solo tutti i singoli bit registrati in esso.

Acquisizione del reperto informatico:

va impedita qualsiasi forma di contaminazione:

- in fase di acquisizione
- durante la conservazione (archiviazione)

va garantita la **chain of custody**

Acquisizione
del reperto informatico:

va accuratamente documentata

per dare garanzia del rispetto dei principi esaminati, tutte le operazioni eseguite in fase di acquisizione vanno accuratamente documentante, meglio se si utilizzando dei dispositivi che registrano automaticamente quanto viene eseguito

Acquisizione
del reperto informatico:

Acquisizione
del reperto informatico:

donato@informaticaforense.it

Acquisizione
del reperto informatico:

donato@informaticaforense.it

Acquisizione
del reperto informatico:

donato@informaticaforense.it

Analisi
del reperto informatico:

Poichè ogni copia coincide con l'originale, l'analisi va eseguita su una copia dei dati acquisiti e non sull'originale

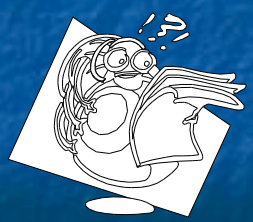
Analisi
del reperto informatico:

- deve essere riproducibile

- ogni singola operazione eseguita sui dati deve produrre sempre lo stesso risultato

Valutazione
del reperto informatico:

Perché è necessario anche un momento di valutazione del reperto, se il bit può assumere solo il valore di 0 o 1 ?



Valutazione
del reperto informatico:

Perché il reperto informatico può essere facilmente:

- alterato
- inquinato
- contraffatto

Valutazione
del reperto informatico:

Inoltre, bisogna verificare se le operazione di acquisizione del reperto informatico sono state legittime

Valutazione
del reperto informatico:

Quindi vanno espressi giudizi di merito circa:
- l'attendibilità
- l'integrità
- l'autenticità

del reperto stesso

Valutazione
del reperto informatico:

integrità

autenticità