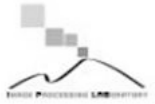





ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA

TECNICHE DI TRATTAMENTO DEI REPERTI INFORMATICI

COMPUTER FORENSICS

CORSO DI LAUREA IN INFORMATICA

ANNO ACCADEMICO 2012- 2013

CATANIA 18 MARZO 2013

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

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….

donato@informaticaforense.it

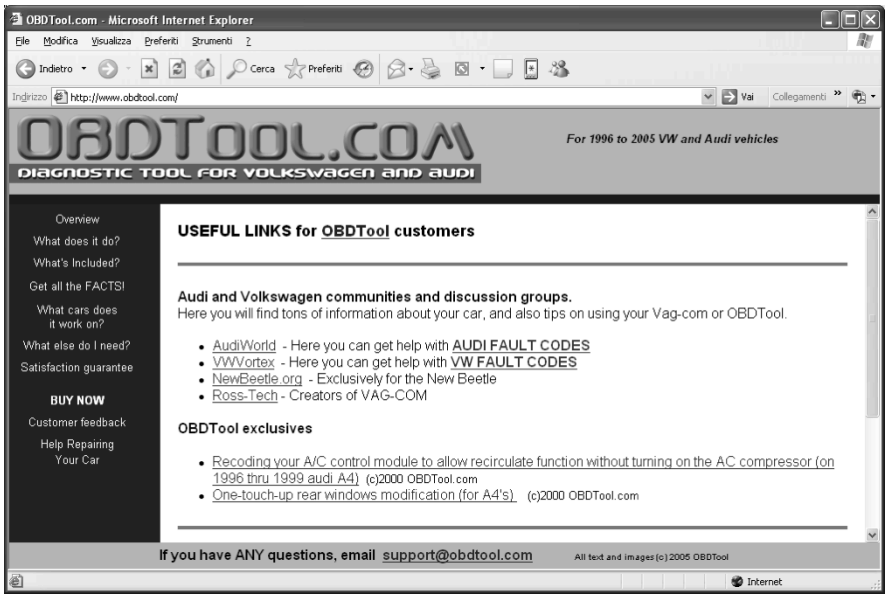
Lista della scansione delle centraline riportante le caratteristiche

Address 01: Engine
Protocol: KWP2000
Part No: 070 906 016 D
Component: V10 5,0L EDCG000AGM 5264
Coding: 0000127
Shop #: WSC 00835

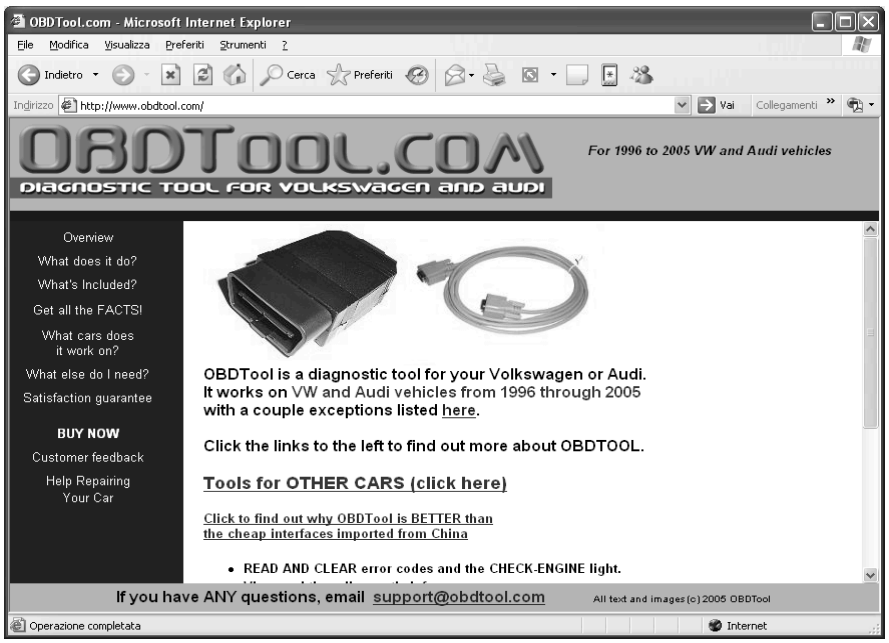
Address 02: Auto Trans
Protocol: KWP2000
Part No: 09D 927 750 E
Component: AL 600 6Q 0318
Coding: 0004136
Shop #: WSC 00835

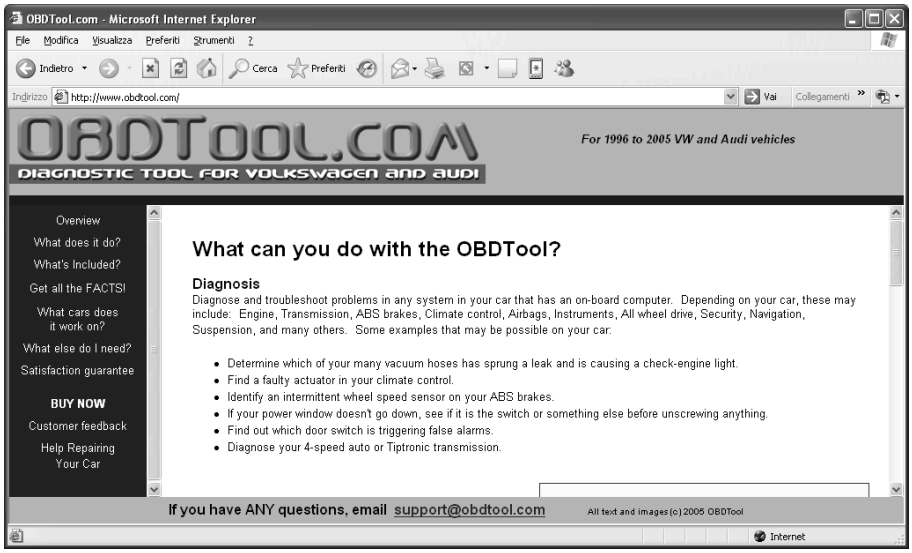
Address 03: ABS Brakes
Protocol: KWP2000
Part No: 7L0 907 379 C
Component: ESP ALLRAD MK25 0107
Coding: 0022785
Shop #: WSC 00835

donato@informaticaforense.it

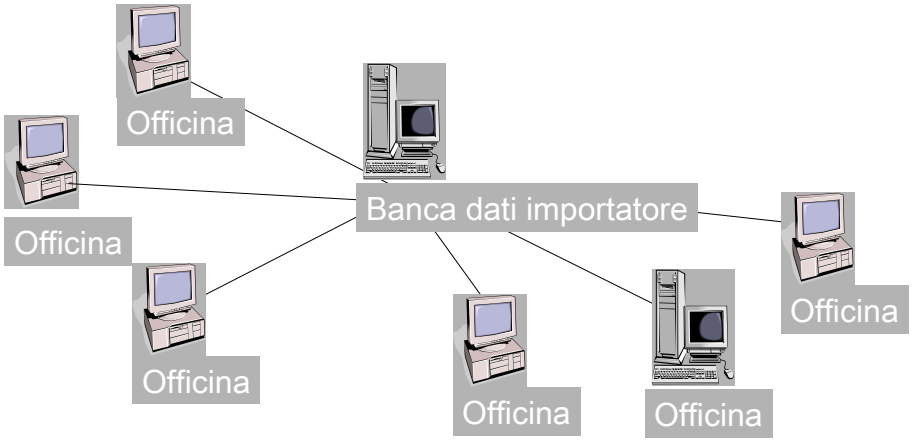


donato@informaticaforense.it


OBDTool.com - Microsoft Internet Explorer
File Modifica Visualizza Preferiti Strumenti ?
Indietro Cerca Preferiti
Indirizzo http://www.obdtool.com/
Vai Collegamenti
OBDTOOL.COM
DIAGNOSTIC TOOL FOR VOLKSWAGEN AND AUDI
For 1996 to 2005 VW and Audi vehicles
Overview
What does it do?
What's Included?
Get all the FACTS!
What cars does it work on?
What else do I need?
Satisfaction guarantee
BUY NOW
Customer feedback
Help Repairing Your Car
OBDTool is a diagnostic tool for your Volkswagen or Audi.
It works on VW and Audi vehicles from 1996 through 2005 with a couple exceptions listed here.
Click the links to the left to find out more about OBDTOOL.
Tools for OTHER CARS (click here)
Click to find out why OBDTool is BETTER than the cheap interfaces imported from China
READ AND CLEAR error codes and the CHECK-ENGINE light.
If you have ANY questions, email support@obdtool.com
All text and images (c) 2005 OBDTool
Operazione completata
Internet


OBDTool.com - Microsoft Internet Explorer
File Modifica Visualizza Preferiti Strumenti ?
Indietro Cerca Preferiti
Indirizzo http://www.obdtool.com/
Vai Collegamenti
OBDTOOL.COM
DIAGNOSTIC TOOL FOR VOLKSWAGEN AND AUDI
For 1996 to 2005 VW and Audi vehicles
Overview
What does it do?
What's Included?
Get all the FACTS!
What cars does it work on?
What else do I need?
Satisfaction guarantee
BUY NOW
Customer feedback
Help Repairing Your Car
What can you do with the OBDTool?
Diagnosis
Diagnose and troubleshoot problems in any system in your car that has an on-board computer. Depending on your car, these may include: Engine, Transmission, ABS brakes, Climate control, Airbags, Instruments, All wheel drive, Security, Navigation, Suspension, and many others. Some examples that may be possible on your car:
Determine which of your many vacuum hoses has sprung a leak and is causing a check-engine light.
Find a faulty actuator in your climate control.
Identify an intermittent wheel speed sensor on your ABS brakes.
If your power window doesn't go down, see if it is the switch or something else before unscrewing anything.
Find out which door switch is triggering false alarms.
Diagnose your 4-speed auto or Tiptronic transmission.
If you have ANY questions, email support@obdtool.com
All text and images (c) 2005 OBDTool
Internet

Lo schema di collegamento delle officine convenzionate



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

donato@informaticaforense.it

Individuazione & marketing

Il datawarehouse…

Accezione forense:

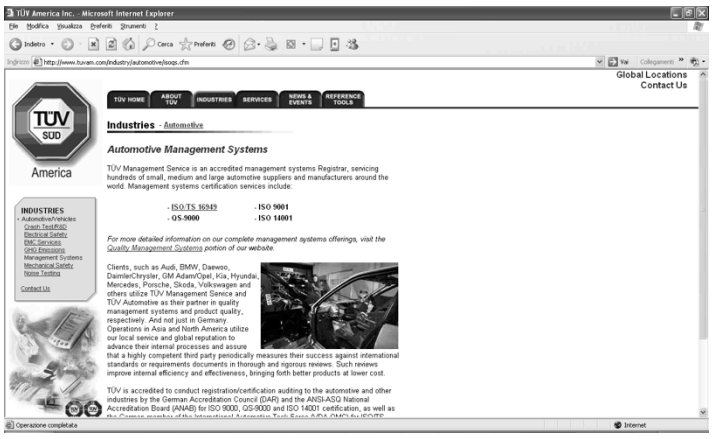
Insieme di dati con elevato valore indiziario

di ampia visibilità facilmente interrogabili..

Es. Un gestore di telefonia…lo vediamo dopo

donato@informaticaforense.it

La certificazione di qualità…



donato@informaticaforense.it

…le conseguenze!

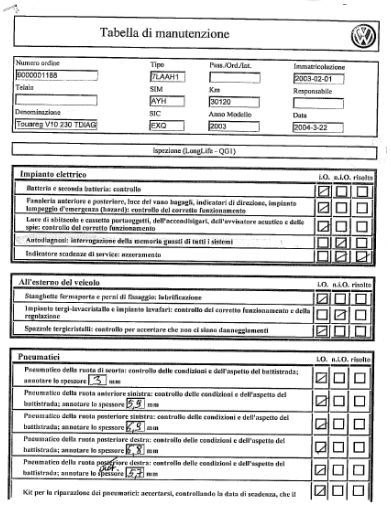


Tabella di manutenzione

Numero ordine	Tipo	Posiz./Ord./Int.	Immatricolazione
8000001188	7LAAH1		2003-02-01
Telaio	SIM	Km	Responsabile
	AYH	30120	
Denominazione	SIC	Anno Modello	Data
Touareg V10 230 TDIAG	EXO	2003	2004-3-22

Ispezione (LongLife - Q01)

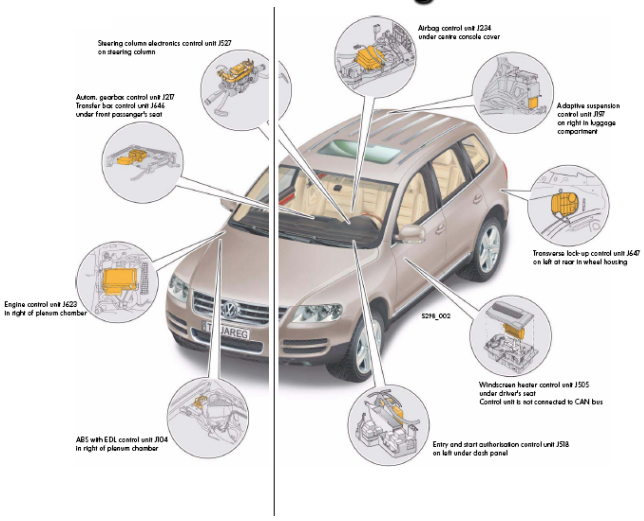
Impianto elettrico	i.O.	n.i.O.	risolto
Batteria e seconda batteria: controllo	☑	☐	☐
Fanaleria anteriore e posteriore, luce del vano bagagli, indicatori di direzione, impianto lampeggio d'emergenza (hazard): controllo del corretto funzionamento	☑	☐	☐
Luce di abitacolo e cassetta portaoggetti, dell'accendisigari, dell'avvisatore acustico e delle spie: controllo del corretto funzionamento	☑	☐	☐
Autodiagnosi: interrogazione della memoria guasti di tutti i sistemi	☐	☑	☐
Indicatore scadenze di service: azzeramento	☐	☑	☐

All'esterno del veicolo	i.O.	n.i.O.	risolto
Stanghette fermaporte e perni di fissaggio: lubrificazione	☑	☐	☐
Impianto tergi-lavacristallo e impianto lavafari: controllo del corretto funzionamento e della regolazione	☐	☑	☐
Spazzole tergicristalli: controllo per accertare che non ci siano danneggiamenti	☑	☐	☐

Pneumatici	i.O.	n.i.O.	risolto
Pneumatico della ruota di scorta: controllo delle condizioni e dell'aspetto del battistrada; annotare lo spessore 5 mm	☑	☐	☐
Pneumatico della ruota anteriore sinistra: controllo delle condizioni e dell'aspetto del battistrada; annotare lo spessore 5,9 mm	☑	☐	☐
Pneumatico della ruota posteriore sinistra: controllo delle condizioni e dell'aspetto del battistrada; annotare lo spessore 6,5 mm	☑	☐	☐
Pneumatico della ruota posteriore destra: controllo delle condizioni e dell'aspetto del battistrada; annotare lo spessore 6,8 mm	☑	☐	☐
Pneumatico della ruota anteriore destra: controllo delle condizioni e dell'aspetto del battistrada; annotare lo spessore 5,2 mm	☑	☐	☐
Kit per la riparazione dei pneumatici: accertarsi, controllando la data di scadenza, che il	☑	☐	☐

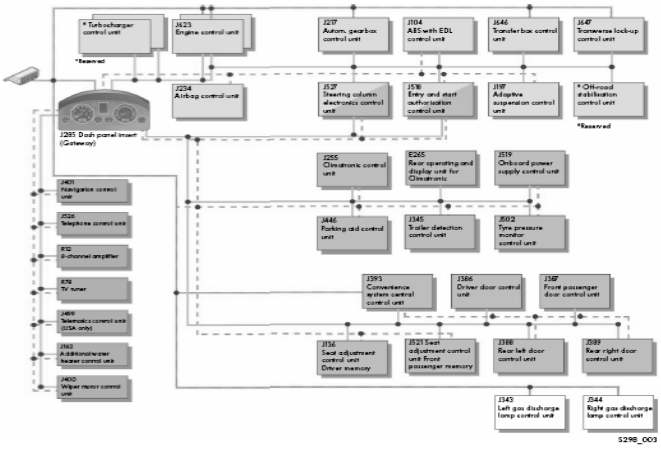
donato@informaticaforense.it

Elenco centraline elettroniche presenti nel Volkswagen Touareg



donato@informaticaforense.it

Elenco centraline elettroniche presenti nel Volkswagen Touareg



donato@informaticaforense.it

donato@informaticaforense.it

Protocollo diagnosi

3 Guasto riconosciuto

00884 002
Indicatore del livello carburante
Valore limite inferiore non raggiunto
guasto fisso

01305 014
Bus dati infotainment
difettoso
guasto fisso

01305 004
Bus dati infotainment
Nessun segnale/nessuna comunicazione
guasto fisso

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:

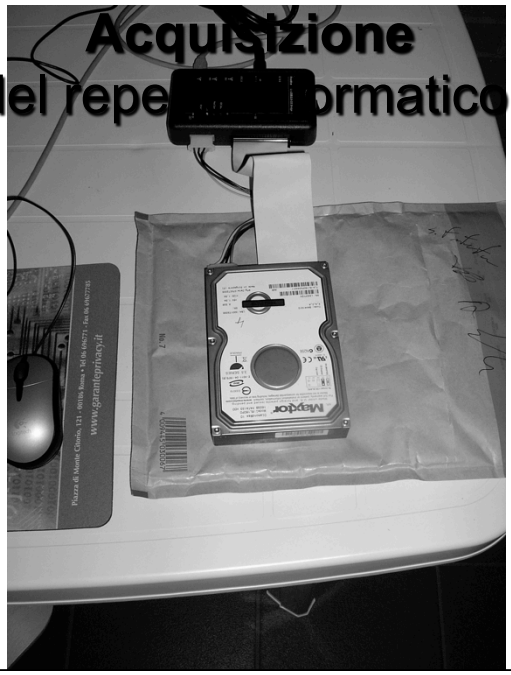
- in fase di acquisizione
- durante la conservazione (archiviazione)

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:

donato@informaticaforense.it

Acquisizione
del reperto informatico:

Acquisizione
del reperto informatico:

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