

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 = 0010100101000101111010101010**

## **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](mailto: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

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

**USEFUL LINKS for OBDTool customers**

**Audi and Volkswagen communities and discussion groups.**  
 Here you will find tons of information about your car, and also tips on using your Vag-com or OBDTool.

- [AudiWorld](#) - Here you can get help with **AUDI FAULT CODES**
- [VWVortex](#) - Here you can get help with **VW FAULT CODES**
- [NewBeetle.org](#) - Exclusively for the New Beetle
- [Ross-Tech](#) - Creators of VAG-COM

**OBDTool exclusives**

- [Recoding your A/C control module to allow recirculate function without turning on the AC compressor \(on 1996 thru 1999 audi A4\)](#) (c)2000 OBDTool.com
- [One-touch-up rear windows modification \(for A4's\)](#). (c)2000 OBDTool.com

If you have ANY questions, email [support@obdtool.com](mailto:support@obdtool.com) All text and images (c) 2005 OBDTool

Internet

donato@informaticaforense.it

OBDDOOL.COM - Microsoft Internet Explorer

File Modifica Visualizza Preferiti Strumenti ?

Indietro

Indirizzo <http://www.obdtool.com/> Vai Collegamenti

# OBDDOOL.COM

For 1996 to 2005 VW and Audi vehicles

DIAGNOSTIC TOOL FOR VOLKSWAGEN AND AUDI

- 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

**OBDDOOL 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 OBDDOOL.**

**Tools for OTHER CARS ([click here](#))**

**[Click to find out why OBDDOOL 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](mailto:support@obdtool.com)** All text and images (c) 2005 OBDDOOL

Operazione completata Internet

[donato@informaticaforense.it](mailto:donato@informaticaforense.it)

OBDDOOL.COM - Microsoft Internet Explorer

File Modifica Visualizza Preferiti Strumenti ?

Indietro

Indirizzo <http://www.obdtool.com/> Vai Collegamenti

# OBDDOOL.COM

For 1996 to 2005 VW and Audi vehicles

DIAGNOSTIC TOOL FOR VOLKSWAGEN AND AUDI

- 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 OBDDOOL?

### 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:

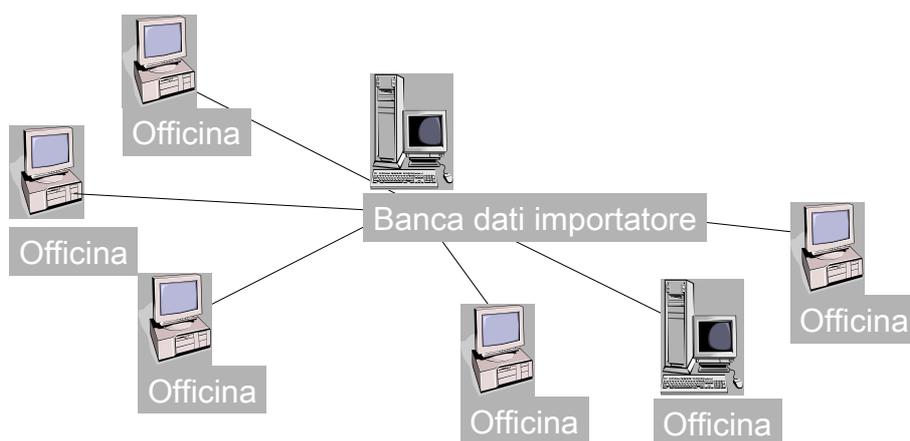
- Determine which of your many vacuum hoses has sprung a leak and is causing a check-engine light.
- Find a faulty actuator in your climate control.
- Identify an intermittent wheel speed sensor on your ABS brakes.
- If your power window doesn't go down, see if it is the switch or something else before 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](mailto:support@obdtool.com)** All text and images (c) 2005 OBDDOOL

Internet

[donato@informaticaforense.it](mailto:donato@informaticaforense.it)

## 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](http://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...

The screenshot shows a web browser window displaying the TUV America Inc. website. The page is titled "Industries - Automotive" and features a navigation menu with links for "HOME", "ABOUT TUV", "INDUSTRIES", "SERVICES", "NEWS & EVENTS", and "REFERENCE TOOLS". The main content area is titled "Automotive Management Systems" and includes a sub-header "Automotive Management Systems". The text describes TUV Management Service as an accredited management systems Registrar, serving hundreds of small, medium and large automotive suppliers and manufacturers around the world. It lists several ISO standards: ISO/TS 16949, ISO 9001, QS-9000, and ISO 14001. A sidebar on the left lists various industries such as Automotive/Vehicles, Cable/Fiber Optic, Chemical, Civil Services, CPU/Electronics, Management Systems, Mechanical/Electrical, and Power/Energy. The page also features a "Global Locations Contact Us" link in the top right corner and a "Operatore completa" link in the bottom left corner.

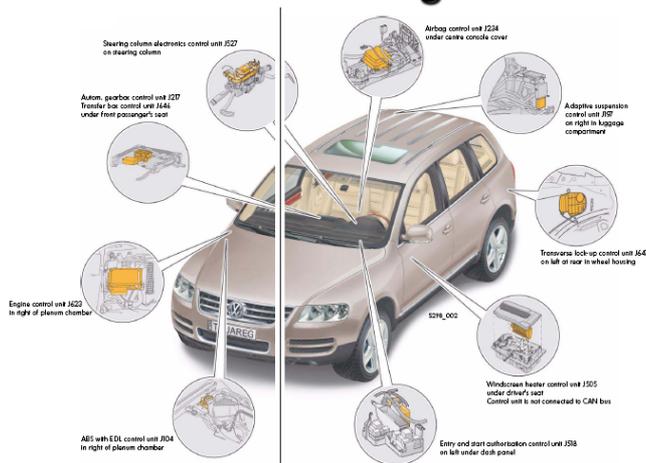
donato@informaticaforense.it

# ...le conseguenze!

| Tabella di manutenzione   |                                     |                                     |                                     |
|---|-------------------------------------|-------------------------------------|-------------------------------------|
| Numero indice   | Tipi                                | Prov. Orig./Est.                    | Immatricolazione                    |
| 000001180   | FLAAT1                              |                                     | 0003-02-01                          |
| Telaio  | SM                                  | Km                                  | Responsabile                        |
|   | RYH                                 | 00120                               |                                     |
| Composizione  | CC                                  | Anno Modello                        | Data                                |
| Touareg V10 330 TDSAG   | FXZ                                 | 2003                                | 0104-3-22                           |
| Specie (LangLife - QCI)   |                                     |                                     |                                     |
| <b>Impianto elettrico</b> I.O. n.L.O. risultato   |                                     |                                     |                                     |
| Batteria e seconda batteria: controllo  | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| Fanaleria anteriore e posteriore, luce dei vasi bagagli, indicatori di direzione, impianto lampadine d'emergenza (batteria): controllo del corretto funzionamento | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| Luce di sblocco e cassette portabagagli, dell'accendisigari, dell'attivatore acustico e delle spie: controllo del corretto funzionamento                          | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| Antifurto: interruzione della corrente, guasti di tutti i circuiti  | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| Indicatore scadenza di servizio: smarrimento  | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| <b>All'esterno del veicolo</b> I.O. n.L.O. risultato  |                                     |                                     |                                     |
| Stanghette fermaporte e paraoli di bloccaggio: lubrificazione   | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| Regolazione degli inverter e impianto lavafari: controllo del corretto funzionamento e della efficienza   | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| Spinele tergicristallo: controllo per accertare che non ci siano danneggiamenti   | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| <b>Pneumatici</b> I.O. n.L.O. risultato   |                                     |                                     |                                     |
| Pneumatico della ruota di servizio: controllo delle condizioni e dell'aspetto del battistrada; assicurare lo spessore di 2 mm                                     | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| Pneumatico della ruota anteriore sinistra: controllo delle condizioni e dell'aspetto del battistrada; assicurare lo spessore di 2 mm                              | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| Pneumatico della ruota posteriore sinistra: controllo delle condizioni e dell'aspetto del battistrada; assicurare lo spessore di 2 mm                             | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| Pneumatico della ruota posteriore destra: controllo delle condizioni e dell'aspetto del battistrada; assicurare lo spessore di 2 mm                               | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| Pneumatico della ruota anteriore destra: controllo delle condizioni e dell'aspetto del battistrada; assicurare lo spessore di 2 mm                                | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| Kit per la riparazione dei pneumatici accertarsi, controllando la data di scadenza, che il  |                                     |                                     |                                     |

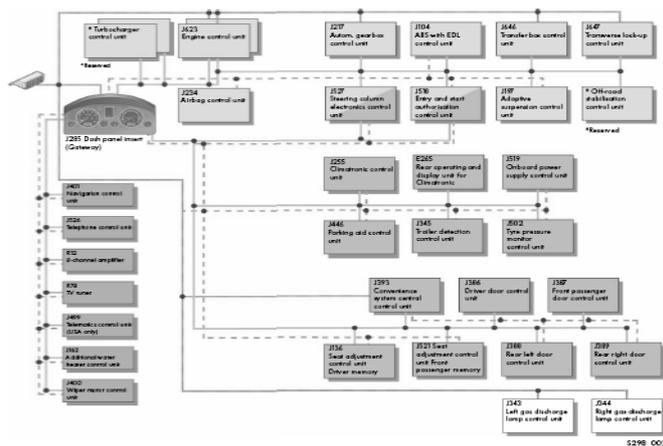
donato@informaticaforense.it

## Elenco centraline elettroniche presenti nel Volkswagen Touareg



donato@informaticaforense.it

## Elenco centraline elettroniche presenti nel Volkswagen Touareg



donato@informaticaforense.it

Home Contatti Link Per i nostri dipendenti [testi da cercare](#)

**Ministero delle Infrastrutture e dei Trasporti**

Magazine **Normativa** Servizi on line **Calendario scorpioni nazionali** **bandi e concorsi** **biblioteca**

sei in: Home page :: trasporto terrestre :: trasporto stradale :: automobili :: veicoli :: albo richiami :: selezione modello :: schede richiami

**Albo dei richiami - 3) visualizzazione dati**

costruttore: Gruppo Volkswagen  
 marca: Volkswagen  
 modello: Touareg

Numero Veicoli: 2791  
 da maggio 2002 a dicembre 2003

Descrizione Difetto: Possibile montaggio bloccetti chiusura diftosi cinture sicurezza posteriori. Possibile montaggio di errate versioni software per motore, cambio automatico, differenziale, sospensione pneumatica. Possibile montaggio differenziali diftosi.

Azioni correttive: verifica ed eventuale sostituzione dei componenti difettosi

Riferimento: 80686579

Note: -

Intervallo testi da: wvg\*\*\*2i\*\*3d00007 \*\*\*4d012314  
 wvg\*\*\*2i\*\*44d0001 \*\*\*4d048017

Il servizio fornisce informazioni su eventuali anomalie riconosciute dalle case costruttrici in base al d.l. n. 78/2000

Tutti i diritti sono del Ministero delle Infrastrutture e dei Trasporti  
 028157042000812 - 23

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 componente 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**

© Donato Eugenio Caccavella

## **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  
documentate, meglio se si utilizzando  
dei dispositivi che registrano  
automaticamente quanto viene eseguito

© Donato Eugenio Caccavella



**Acquisizione  
del reperto informatico:**



donato@informicaforense.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 ?

© Donato Eugenio Caccavella

## **Valutazione del reperto informatico:**

Perché il reperto informatico può essere facilmente:

- alterato
- inquinato
- contraffatto

**Valutazione  
del reperto informatico:**

Inoltre, bisogna verificare  
se le operazioni 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