ON THE DIGITAL FORENSICS OF HEAVY TRUCK ELECTRONIC CONTROL MODULES

James Johnson, Jeremy Daily, and Andrew Kongs

The University of Tulsa

SAE INTERNATIONAL

THE UNIVERSITY of TULSA

Department of Mechanical Engineering

Introduction and Overview

Problem Definition

Digital Forensics Concepts and Forensic Soundness

Applications to HVEDRs

Examples from Detroit Diesel and DDEC Reports

Chip Level Forensics

Problem Statement

Scenarios:

1. **Company Safety Director downloads a drivable truck then puts the truck back in service.**
2. **Multiple attorneys, experts, videographers stand around and watch someone capture screenshots for a couple hours. (Not possible for Law Enforcement)**

Issues:

1. **A conflicted party is the sole possessor of the data.**
2. **Many people are needed to verify data is authentic.**

These are examples with many more possibilities…

Core Issue of Trust

The meaning, relevance, trustworthiness and admissibility of digital data from an ECM may be contested in court.

Establishing trust for Personal Computer Hard Drives is well established.

OEM software native file formats are not secure.

Tampering with file contents can be undetectable.

Forensic Soundness

Establish a notion of trust for the courts to qualify and justify for information derived from digital data.

1. **Meaning**
   Confidence in the interpretation
2. **Error Detection and Prediction**
   Understanding what can change in the forensic process
3. **Transparency**
   Process is known, documented and verifiable
4. **Expertise**
   Personnel are qualified
5. **Data Integrity and Tamper Resistance**
   Data alterations are detected

Digital Investigation
Advances in Digital Forensics IV
Edited by Indrajit Ray Sujeet Shenoi
Springer
ifip
NIJ
Special REPORT
Electronic Crime Scene Investigation:
A Guide for First Responders, Second Edition

Meaning Applied to HVEDRs

Standards Based Meaning

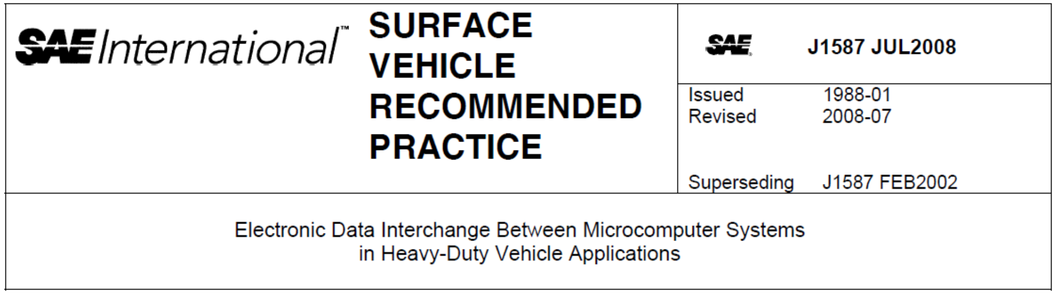
- **SAE J1587**

A.84 ROAD SPEED

Indicated vehicle velocity.

Parameter Data Length: 1 Character
Data Type: Unsigned Short Integer
Bit Resolution: 0.805 km/h (0.5 mph)
Maximum Range: 0.0 to 205.2 km/h (0.0 to 127.5 mph)
Transmission Update Period: 0.1 s
Message Priority: 1
Format:

PID	Data
84	a
a—	Road speed



SAE International™ SURFACE VEHICLE RECOMMENDED PRACTICE

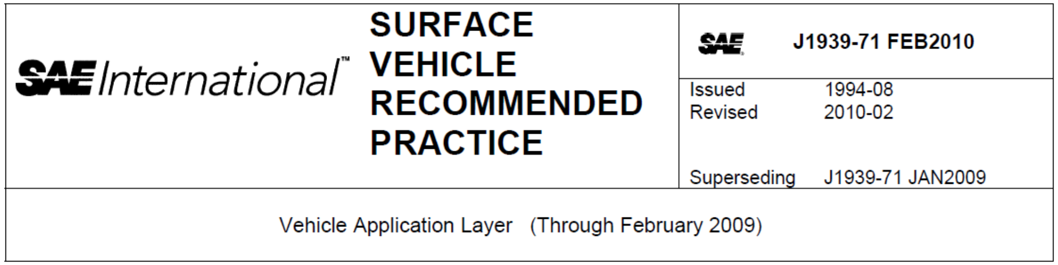
SAE J1587 JUL2008

Issued 1988-01
Revised 2008-07

Superseding J1587 FEB2002

Electronic Data Interchange Between Microcomputer Systems
in Heavy-Duty Vehicle Applications

- **SAE J1939-71**
- **SAE J1939-73**



SAE International™ SURFACE VEHICLE RECOMMENDED PRACTICE

SAE J1939-71 FEB2010

Issued 1994-08
Revised 2010-02

Superseding J1939-71 JAN2009

Vehicle Application Layer (Through February 2009)

Meaning Applied to HVEDRs (Cont.)

Proprietary Software Interpretation

ECM Family	Software
Caterpillar	Caterpillar Electronic Technician (CatET)
Cummins	Cummins PowerSpec Cummins Insite
Detroit Diesel	DDEC Reports Detroit Diesel Diagnostic Link (DDDL)
Navistar	ServiceMaxx

Research shows that OEM software should be independently verified.

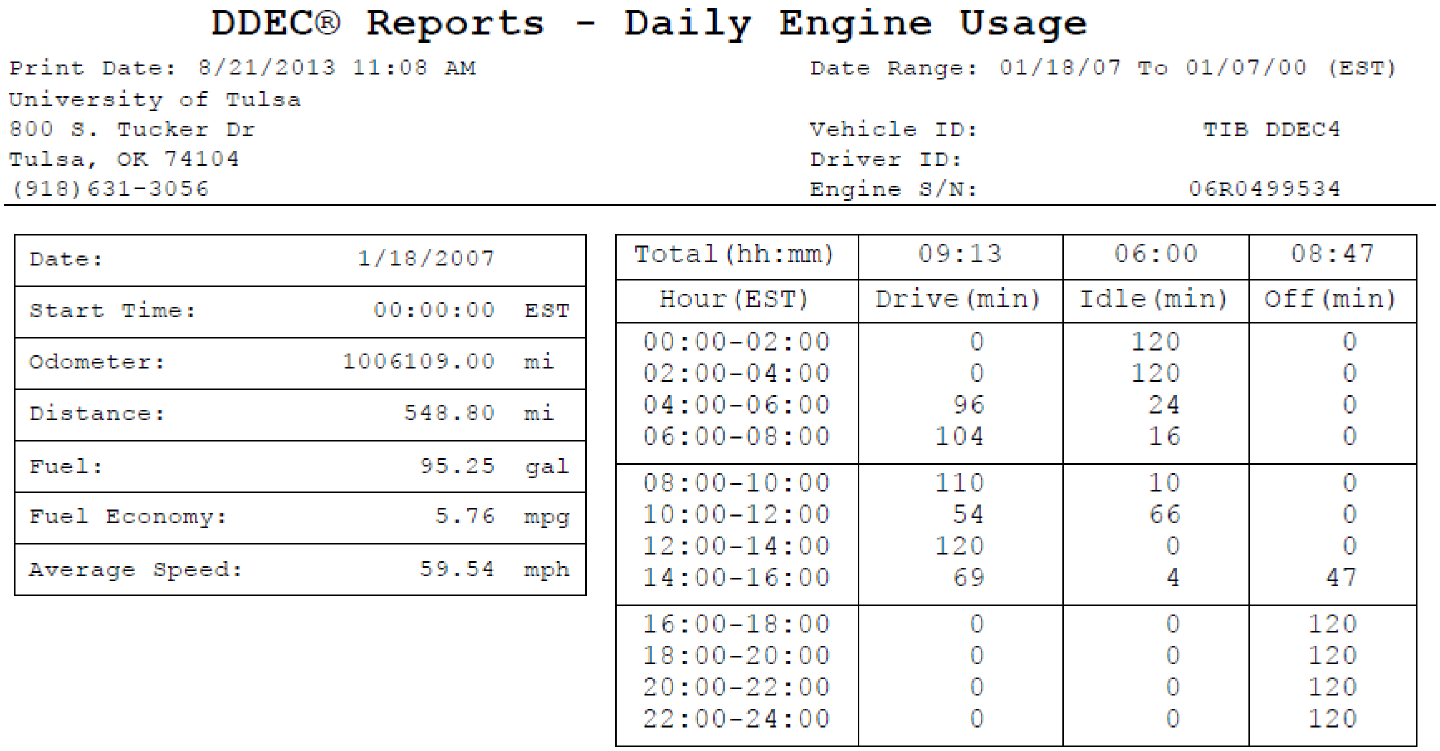
For example:

- **Caterpillar Snapshot Intervals (Austin, 2011-01-0807)**
- **Cummins Sudden Deceleration Timing (Bortolin, 2009-01-0876)**

Daily Engine Usage from DDEC Reports

Goal: Help understand meaning by examining the digital record.

What data actually exists in the record?



DDEC® Reports - Daily Engine Usage

Print Date: 8/21/2013 11:08 AM
University of Tulsa
800 S. Tucker Dr
Tulsa, OK 74104
(918)631-3056

Date Range: 01/18/07 To 01/07/00 (EST)

Vehicle ID: TIB DDEC4
Driver ID:
Engine S/N: 06R0499534

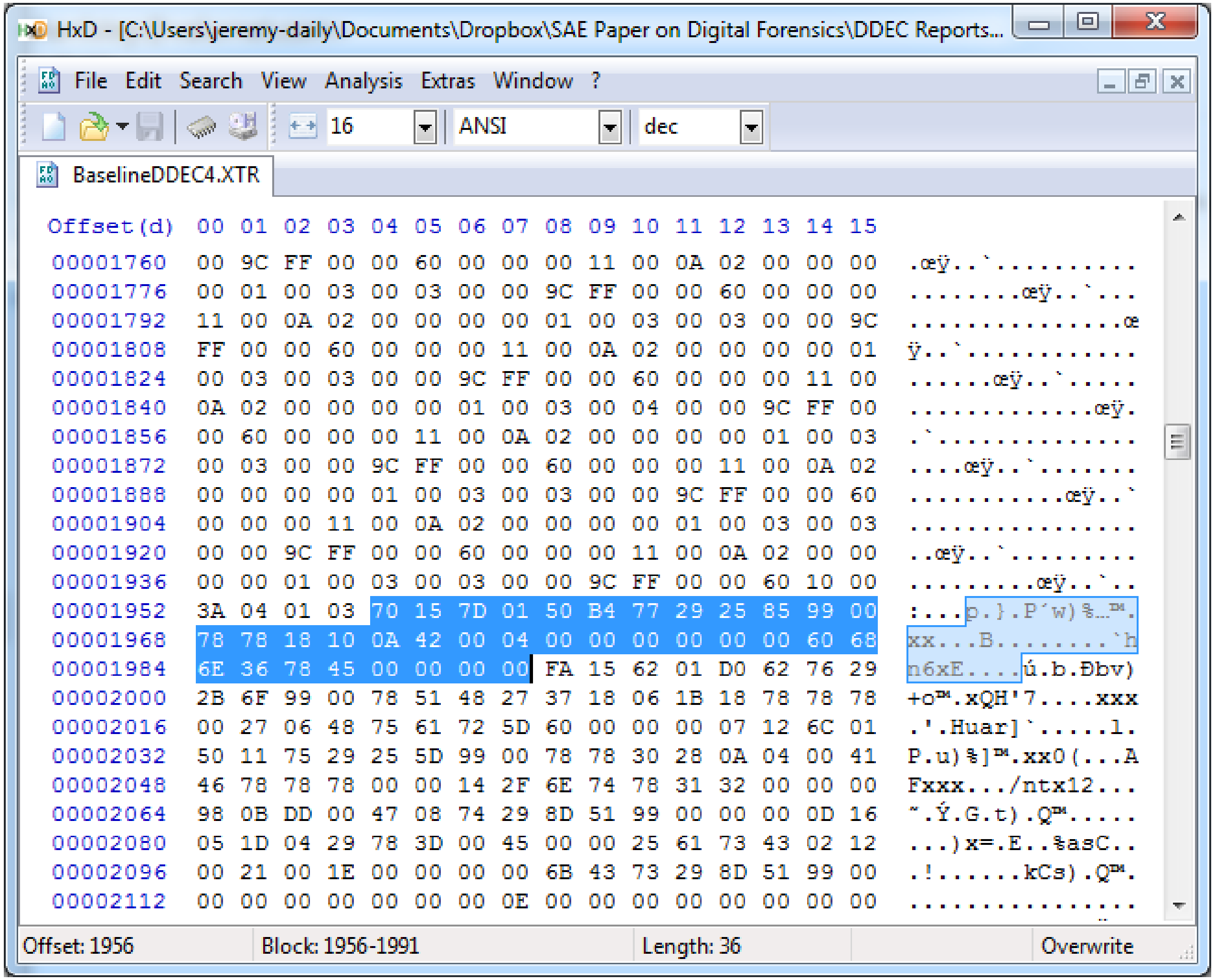
Date:	1/18/2007	
Start Time:	00:00:00	EST
Odometer:	1006109.00	mi
Distance:	548.80	mi
Fuel:	95.25	gal
Fuel Economy:	5.76	mpg
Average Speed:	59.54	mph

Total(hh:mm)	09:13	06:00	08:47
Hour(EST)	Drive(min)	Idle(min)	Off(min)
00:00-02:00	0	120	0
02:00-04:00	0	120	0
04:00-06:00	96	24	0
06:00-08:00	104	16	0
08:00-10:00	110	10	0
10:00-12:00	54	66	0
12:00-14:00	120	0	0
14:00-16:00	69	4	47
16:00-18:00	0	0	120
18:00-20:00	0	0	120
20:00-22:00	0	0	120
22:00-24:00	0	0	120

DDEC Reports data are in the .XTR file.

Daily Engine Usage from DDEC Reports

DDEC Reports .XTR file in a Hex Editor



HxD - [C:\Users\jeremy-daily\Documents\Dropbox\SAE Paper on Digital Forensics\DDEC Reports...
File Edit Search View Analysis Extras Window ?
BaselineDDEC4.XTR

16 | ANSI | dec

```
Offset(d) 00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15

00001760  00 9C FF 00 00 60 00 00 00 11 00 0A 02 00 00 00  .œÿ..`..........
00001776  00 01 00 03 00 03 00 00 9C FF 00 00 60 00 00 00  ........œÿ..`...
00001792  11 00 0A 02 00 00 00 00 01 00 03 00 03 00 00 9C  ...............œ
00001808  FF 00 00 60 00 00 00 11 00 0A 02 00 00 00 00 01  ÿ..`............
00001824  00 03 00 03 00 00 9C FF 00 00 60 00 00 00 11 00  ......œÿ..`.....
00001840  0A 02 00 00 00 00 01 00 03 00 04 00 00 9C FF 00  .............œÿ.
00001856  00 60 00 00 00 11 00 0A 02 00 00 00 00 01 00 03  .`..............
00001872  00 03 00 00 9C FF 00 00 60 00 00 00 11 00 0A 02  ....œÿ..`.......
00001888  00 00 00 00 01 00 03 00 03 00 00 9C FF 00 00 60  ...........œÿ..`
00001904  00 00 00 11 00 0A 02 00 00 00 00 01 00 03 00 03  ................
00001920  00 00 9C FF 00 00 60 00 00 00 11 00 0A 02 00 00  ..œÿ..`.........
00001936  00 00 01 00 03 00 03 00 00 9C FF 00 00 60 10 00  .........œÿ..`..
00001952  3A 04 01 03 70 15 7D 01 50 B4 77 29 25 85 99 00  :...p.}.P´w)%…™.
00001968  78 78 18 10 0A 42 00 04 00 00 00 00 00 00 60 68  xx...B........`h
00001984  6E 36 78 45 00 00 00 00 FA 15 62 01 D0 62 76 29  n6xE....ú.b.Ðbv)
00002000  2B 6F 99 00 78 51 48 27 37 18 06 1B 18 78 78 78  +o™.xQH'7....xxx
00002016  00 27 06 48 75 61 72 5D 60 00 00 00 07 12 6C 01  .'.Huar]`.....l.
00002032  50 11 75 29 25 5D 99 00 78 78 30 28 0A 04 00 41  P.u)%]™.xx0(...A
00002048  46 78 78 78 00 00 14 2F 6E 74 78 31 32 00 00 00  Fxxx.../ntx12...
00002064  98 0B DD 00 47 08 74 29 8D 51 99 00 00 00 0D 16  ˜.Ý.G.t).Q™.....
00002080  05 1D 04 29 78 3D 00 45 00 00 25 61 73 43 02 12  ...)x=.E..%asC..
00002096  00 21 00 1E 00 00 00 00 6B 43 73 29 8D 51 99 00  .!......kCs).Q™.
00002112  00 00 00 00 00 00 00 0E 00 00 00 00 00 00 00 00  ................
```

Offset: 1956 | Block: 1956-1991 | Length: 36 | Overwrite

Daily Engine Usage from DDEC Reports

Interpreted Data

Bytes Sequence	Hex Value (s)	Decimal	LSB Value	Meaning	Value
0-1	70 15	5488	0.1 mile	Distance	548.8 miles
2-3	7D 01	381	0.25 gal	Fuel	95.25 gallons
4-7	50 B4 77 29	695710800	1 sec from epoch	Start Time	17 Jan 2007 at 23:00:00 CST
8-11	25 85 99 00	10061093	0.1 mile	Odometer	1006109.3 miles
12-23	78 78 18 10 0A 42 00 04 00 00 00 00	120 120 24 16 10 66 0 4 0 0 0 0	1 Minute	Idle Time	Same as Decimal
24-35	00 00 60 68 6E 36 78 45 00 00 00 00	0 0 96 104 54 120 69 0 0 0 0	1 Minute	Drive Time	Same as Decimal

All other data are calculated.

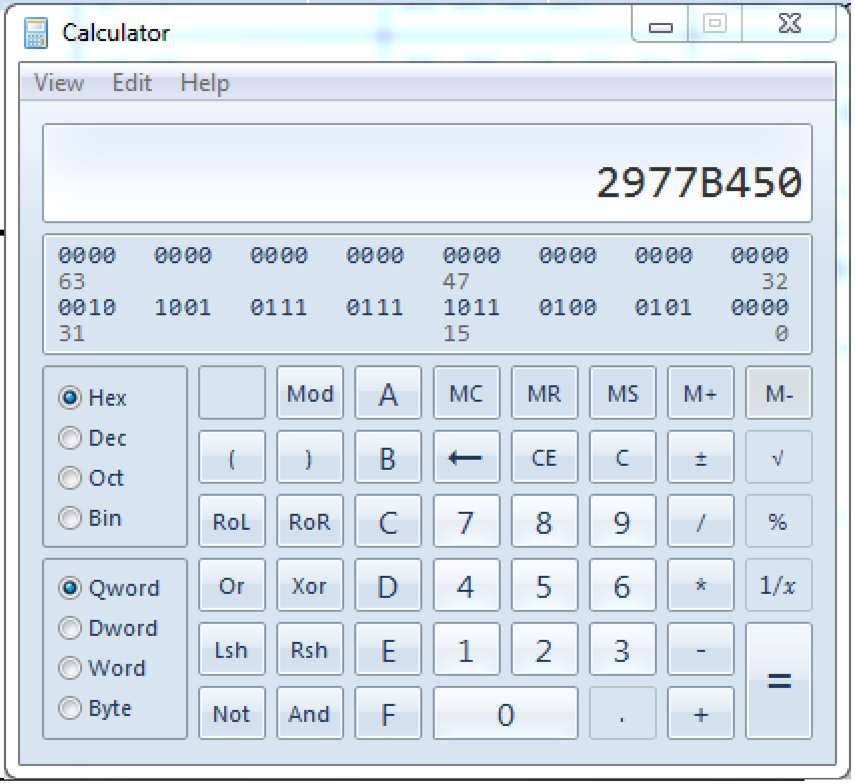
.XTR file contains minutes, but the chip memory contains seconds.

DDEC Reports Time Stamps

Understanding Time Stamps – Obtaining time from Hex

Bytes Sequence	Hex Value (s)	Decimal	LSB Value	Meaning	Value
4-7	50 B4 77 29	695710800	1 sec from epoch	Start Time	17 Jan 2007 at 23:00:00 CST

1. **Convert Hex to Decimal**
   Encoded as a 4 byte (32 bit) integer in Intel format (little endian).
   a) Byte swap to Motorola Format (big endian)
      0x29 0x77 0xB4 0x50
   b) Convert to Decimal with Windows Calculator



2977B450

```
0000   0000   0000   0000   0000   0000   0000   0000
63                          47                     32
0010   1001   0111   0111   1011   0100   0101   0000
31                          15                      0
```

● Hex
○ Dec
○ Oct
○ Bin

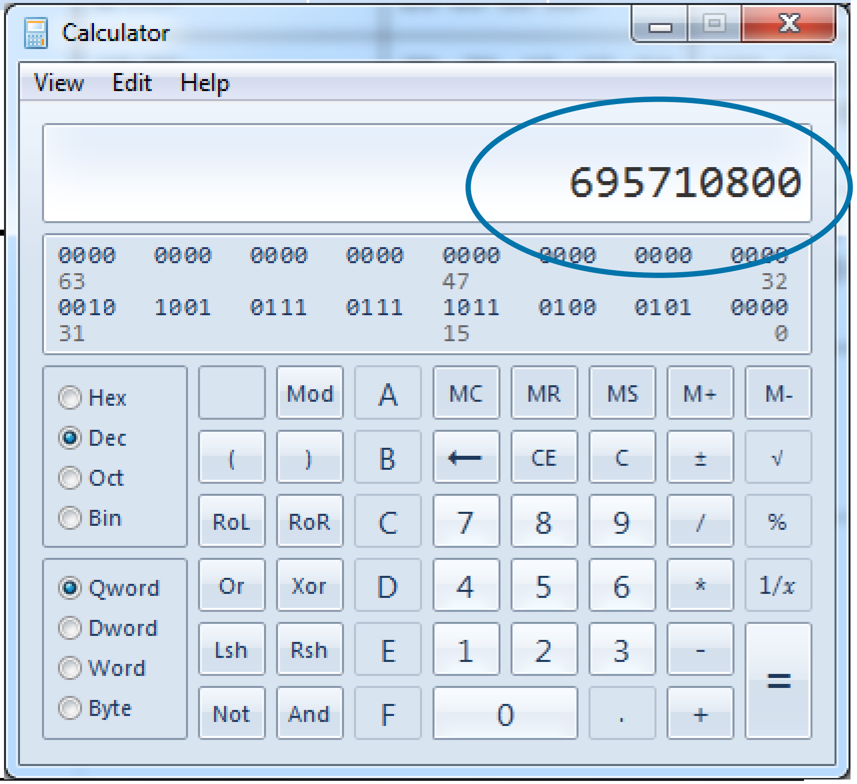
● Qword
○ Dword
○ Word
○ Byte

DDEC Reports Time Stamps

Understanding Time Stamps – Obtaining time from Hex

Bytes Sequence	Hex Value (s)	Decimal	LSB Value	Meaning	Value
4-7	50 B4 77 29	695710800	1 sec from epoch	Start Time	17 Jan 2007 at 23:00:00 CST

1. **Convert Hex to Decimal**
   Encoded as a 4 byte (32 bit) integer in Intel format (little endian).
   a) Byte swap to Motorola Format (big endian)
   0x29 0x77 0xB4 0x50
   b) Convert to Decimal with Windows Calculator



```
695710800
```

```
0000 0000 0000 0000 0000 0000 0000 0000
63                  47                  32
0010 1001 0111 0111 1011 0100 0101 0000
31                  15                   0
```

○ Hex
● Dec
○ Oct
○ Bin

● Qword
○ Dword
○ Word
○ Byte

What does the big number mean?

DDEC Reports Time Stamps

SAE J1587 and J1939 recommend the epoch to be

00:00:00 on 01 Jan 1985 UTC

or

19:00:00 on 31 Dec 1984 Eastern Time

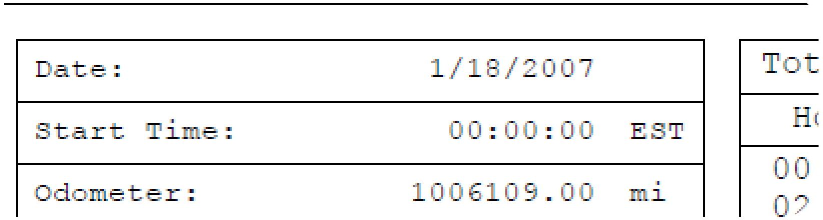
Computer epoch is 00:00:00 on 01 Jan 1970 UTC

15 year offset = 473,364,000 seconds.

Add 473,364,000 seconds to 695,710,800 seconds and convert

```
>>> print(time.strftime("%A, %d %b %Y at %H:%M:%S %Z",
                        time.gmtime(473364000 + 695710800 )))
```

Wednesday, 17 Jan 2007 at 23:00:00 Central Standard Time



Date:	1/18/2007	
Start Time:	00:00:00	EST
Odometer:	1006109.00	mi

Tot

H(

00

02

Data Integrity

File formats are vulnerable to alteration

- Cummins PowerSpec: plaintext HTML
- DDEC Reports: .XTR binary reflects unencrypted network traffic

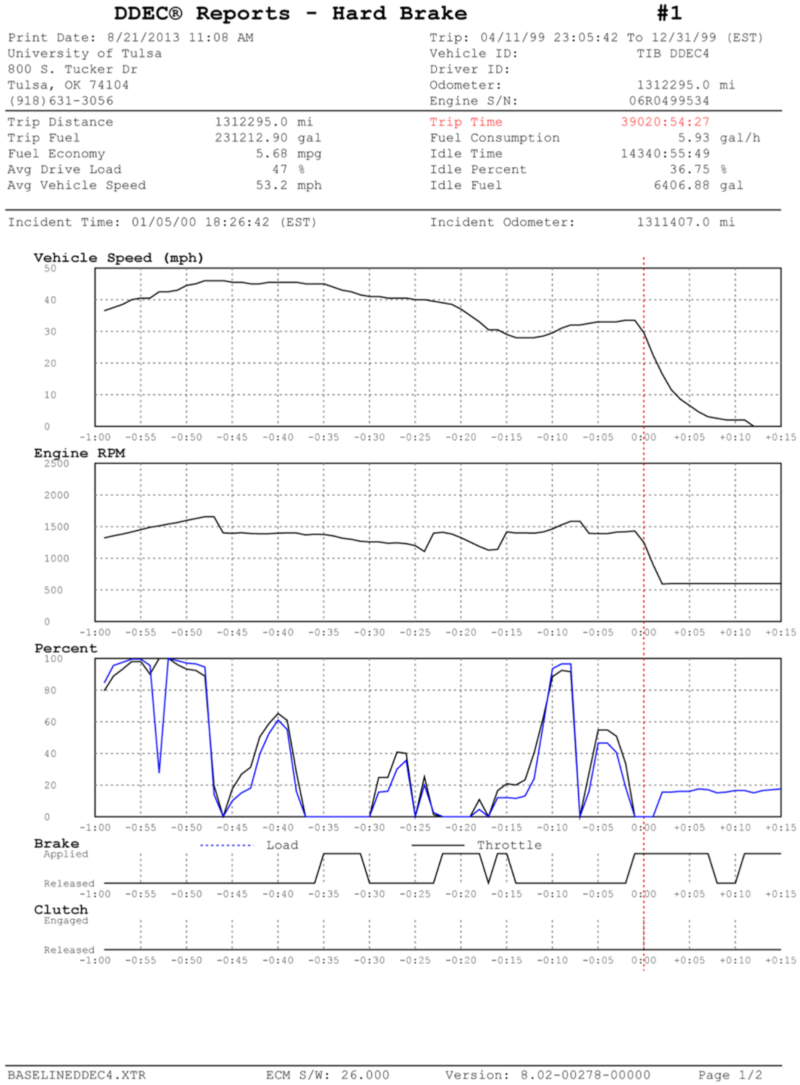
Current software has no hashing or checksum to detect alteration

- Bosch CDR Tool has a CRC-32 checksum (at least it's something).
- SAE J2728 recommends a "verification file" to store a computed verification value.

Alteration can be detected using a Cryptographic Hash Function

http://en.wikipedia.org/wiki/Cryptographic_hash_function

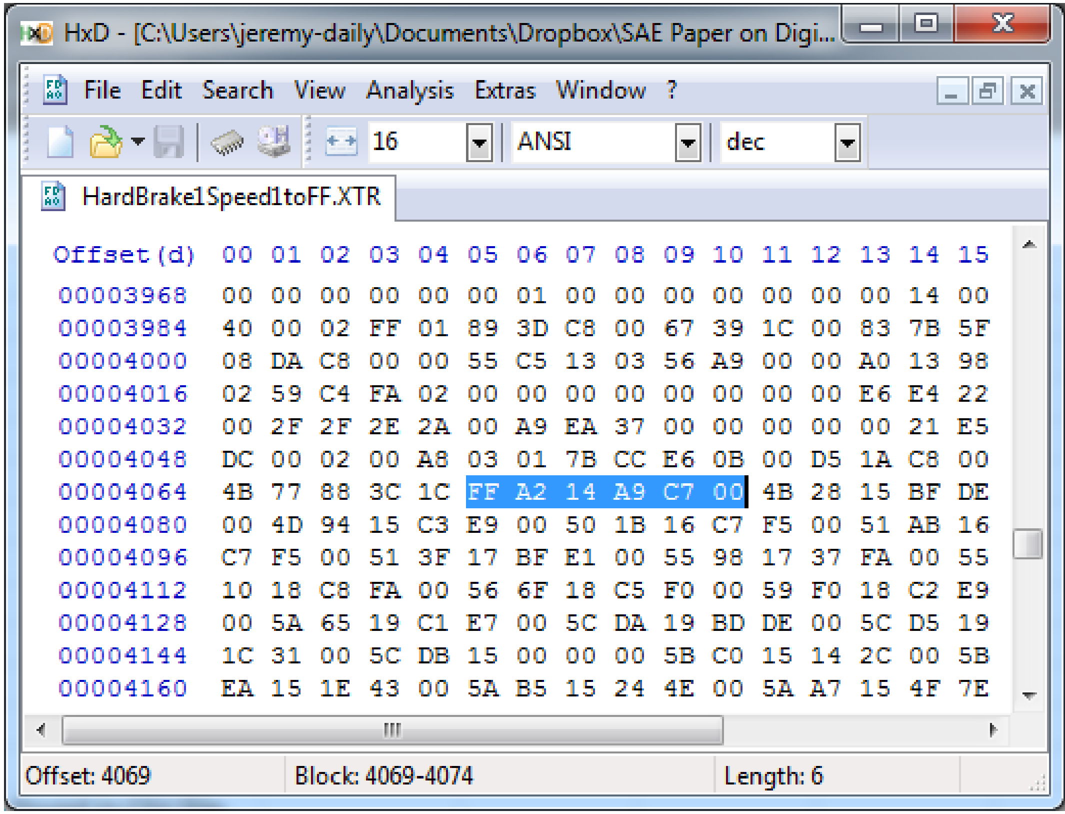
Altering DDEC Reports .XTR file



```
            DDEC® Reports - Hard Brake                    #1
Print Date: 8/21/2013 11:08 AM               Trip: 04/11/99 23:05:42 To 12/31/99 (EST)
University of Tulsa                          Vehicle ID:            TIB DDEC4
800 S. Tucker Dr                             Driver ID:
Tulsa, OK 74104                              Odometer:              1312295.0 mi
(918)631-3056                                Engine S/N:           06R0499534
Trip Distance            1312295.0 mi        Trip Time             39020:54:27
Trip Fuel                231212.90 gal       Fuel Consumption             5.93 gal/h
Fuel Economy                  5.68 mpg       Idle Time             14340:55:49
Avg Drive Load                  47 %         Idle Percent                36.75 %
Avg Vehicle Speed             53.2 mph       Idle Fuel                 6406.88 gal

Incident Time: 01/05/00 18:26:42 (EST)       Incident Odometer:     1311407.0 mi
```

```
BASELINEDDEC4.XTR          ECM S/W: 26.000        Version: 8.02-00278-00000        Page 1/2
```

First entry in Hard Brake #1 highlighted.
Change the Speed Byte to 0xFF



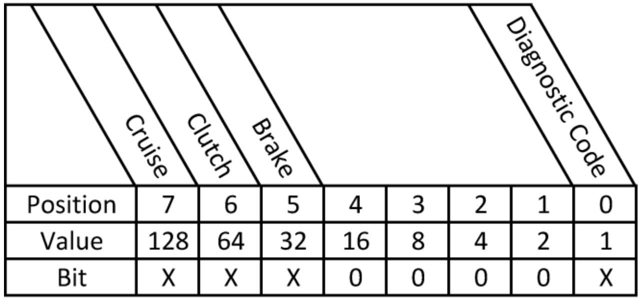
```
Offset(d)  00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15

00003968   00 00 00 00 00 00 01 00 00 00 00 00 00 00 14 00
00003984   40 00 02 FF 01 89 3D C8 00 67 39 1C 00 83 7B 5F
00004000   08 DA C8 00 00 55 C5 13 03 56 A9 00 00 A0 13 98
00004016   02 59 C4 FA 02 00 00 00 00 00 00 00 00 E6 E4 22
00004032   00 2F 2F 2E 2A 00 A9 EA 37 00 00 00 00 00 21 E5
00004048   DC 00 02 00 A8 03 01 7B CC E6 0B 00 D5 1A C8 00
00004064   4B 77 88 3C 1C FF A2 14 A9 C7 00 4B 28 15 BF DE
00004080   00 4D 94 15 C3 E9 00 50 1B 16 C7 F5 00 51 AB 16
00004096   C7 F5 00 51 3F 17 BF E1 00 55 98 17 37 FA 00 55
00004112   10 18 C8 FA 00 56 6F 18 C5 F0 00 59 F0 18 C2 E9
00004128   00 5A 65 19 C1 E7 00 5C DA 19 BD DE 00 5C D5 19
00004144   1C 31 00 5C DB 15 00 00 00 5B C0 15 14 2C 00 5B
00004160   EA 15 1E 43 00 5A B5 15 24 4E 00 5A A7 15 4F 7E
```

Offset: 4069   Block: 4069-4074   Length: 6

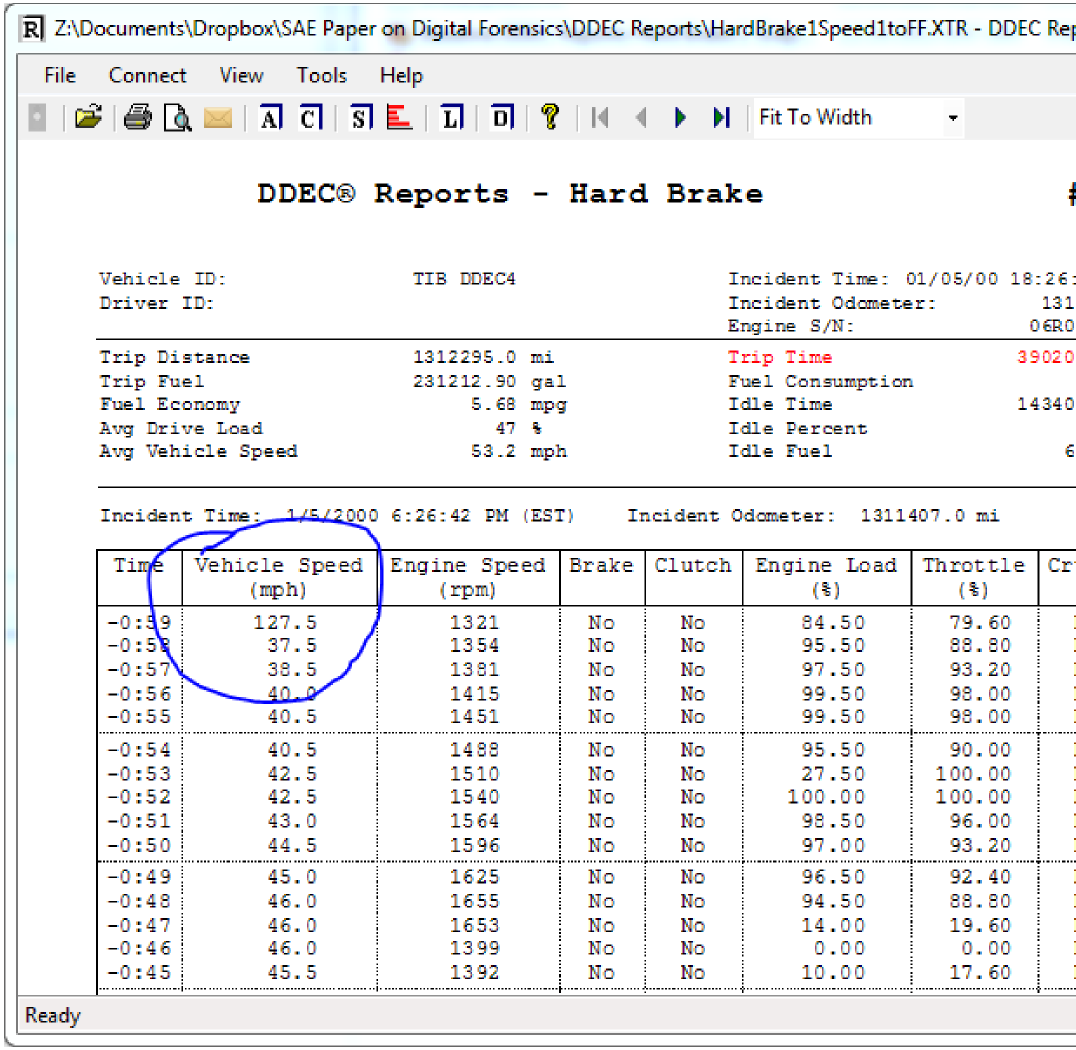
DDEC Reports had no problem reopening a file after manipulating the data.

Most bytes can be mapped to fields within DDEC Reports.

Example: Switch data.



Position	7	6	5	4	3	2	1	0
Value	128	64	32	16	8	4	2	1
Bit	X	X	X	0	0	0	0	X



Z:\Documents\Dropbox\SAE Paper on Digital Forensics\DDEC Reports\HardBrake1Speed1toFF.XTR - DDEC Rep

DDEC® Reports - Hard Brake

```
Vehicle ID:          TIB DDEC4                 Incident Time:  01/05/00 18:26:
Driver ID:                                     Incident Odometer:          131
                                               Engine S/N:                06R0
Trip Distance        1312295.0 mi              Trip Time                  39020
Trip Fuel            231212.90 gal             Fuel Consumption
Fuel Economy              5.68 mpg             Idle Time                  14340
Avg Drive Load              47 %               Idle Percent
Avg Vehicle Speed         53.2 mph             Idle Fuel                      6

Incident Time:  1/5/2000 6:26:42 PM (EST)    Incident Odometer:  1311407.0 mi
```

Time	Vehicle Speed (mph)	Engine Speed (rpm)	Brake	Clutch	Engine Load (%)	Throttle (%)	Cr
-0:59	127.5	1321	No	No	84.50	79.60	
-0:58	37.5	1354	No	No	95.50	88.80	
-0:57	38.5	1381	No	No	97.50	93.20	
-0:56	40.0	1415	No	No	99.50	98.00	
-0:55	40.5	1451	No	No	99.50	98.00	
-0:54	40.5	1488	No	No	95.50	90.00	
-0:53	42.5	1510	No	No	27.50	100.00	
-0:52	42.5	1540	No	No	100.00	100.00	
-0:51	43.0	1564	No	No	98.50	96.00	
-0:50	44.5	1596	No	No	97.00	93.20	
-0:49	45.0	1625	No	No	96.50	92.40	
-0:48	46.0	1655	No	No	94.50	88.80	
-0:47	46.0	1653	No	No	14.00	19.60	
-0:46	46.0	1399	No	No	0.00	0.00	
-0:45	45.5	1392	No	No	10.00	17.60	

SOLUTIONS:

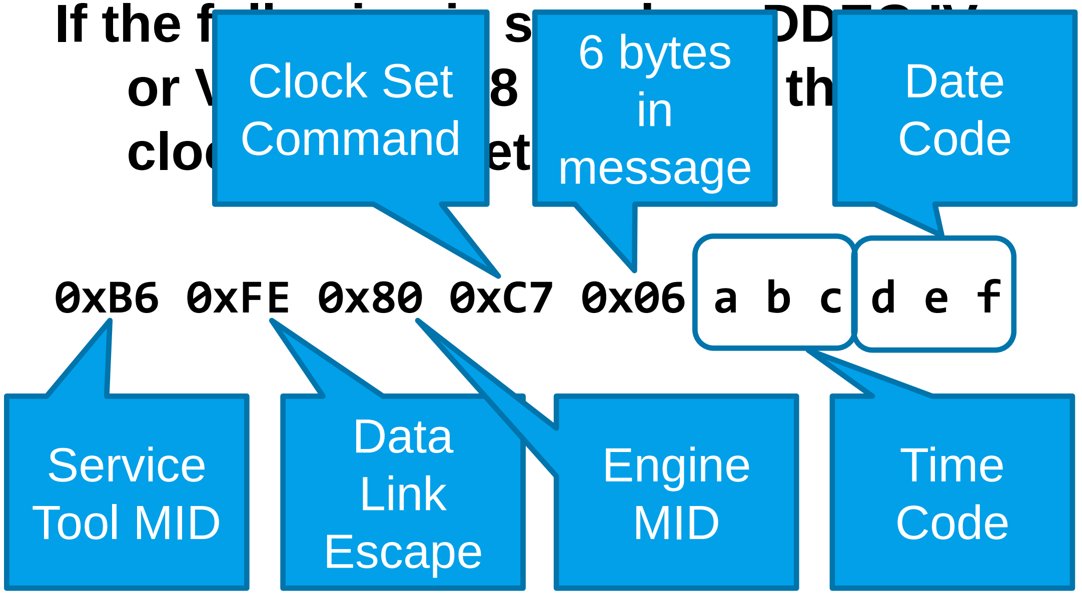
DIGITAL FORENSICS CONCEPTS FOR HVEDRS

Write Blocking

Some messages from diagnostic software affect data on ECM

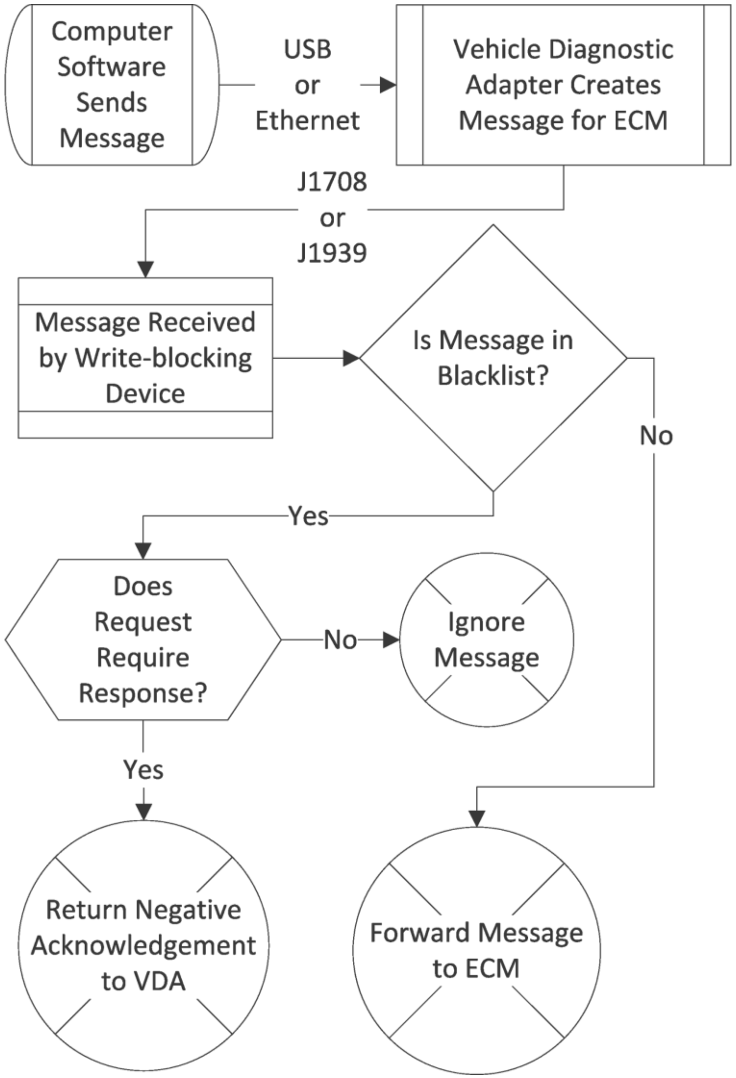
Example: DDEC ECM Clock Set

If the f s DD or V 8 th cloc et



```
0xB6 0xFE 0x80 0xC7 0x06 a b c d e f
```

Message should be blocked.

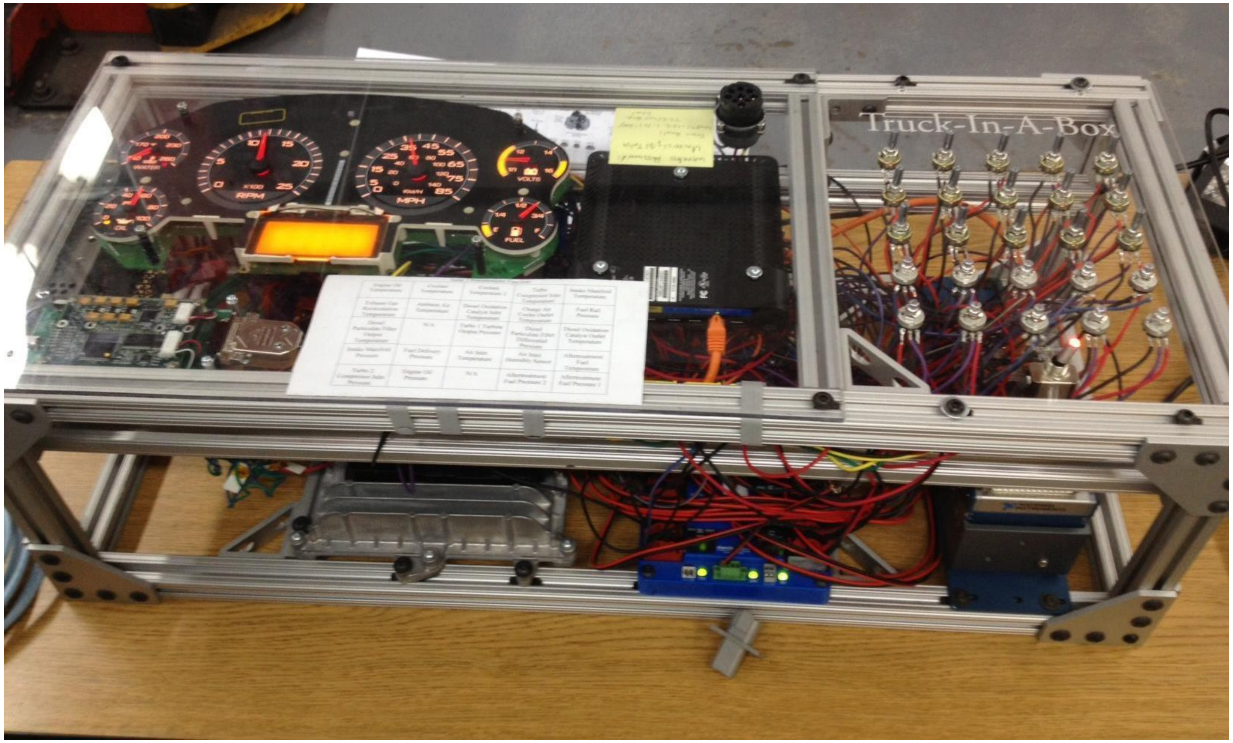


Computer Software Sends Message
USB or Ethernet
Vehicle Diagnostic Adapter Creates Message for ECM
J1708 or J1939
Message Received by Write-blocking Device
Is Message in Blacklist?
No
Yes
Does Request Require Response?
No
Ignore Message
Yes
Return Negative Acknowledgement to VDA
Forward Message to ECM

Avoid Writing New Fault Codes

Sensor Simulators make the ECM think it is still in a vehicle.

- **Passive Signals (e.g. Voltage Dividers**
- **Active Signals (e.g. Accelerator Pedal Position pulses)**
- **Network Signals (e.g. Transmission Control Message on J1939)**

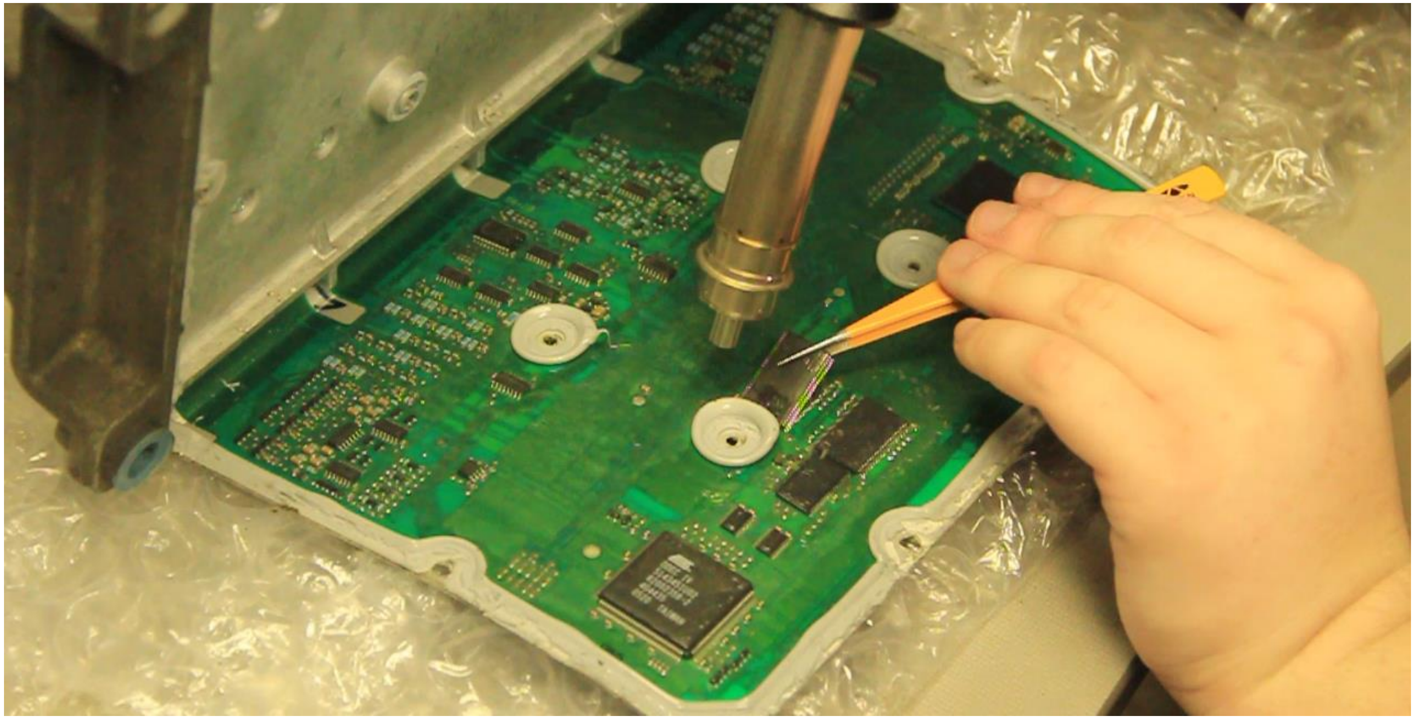


Caution: Different configurations (VINs) may give different fault codes.

Chip Level Forensics

Examine the data in the memory storage devices using a chip reader.

- DDEC V Daily Engine Usage Logs are stored in seconds.
- DDEC Reports data is in different places in physical memory.



Strong Data Encryption

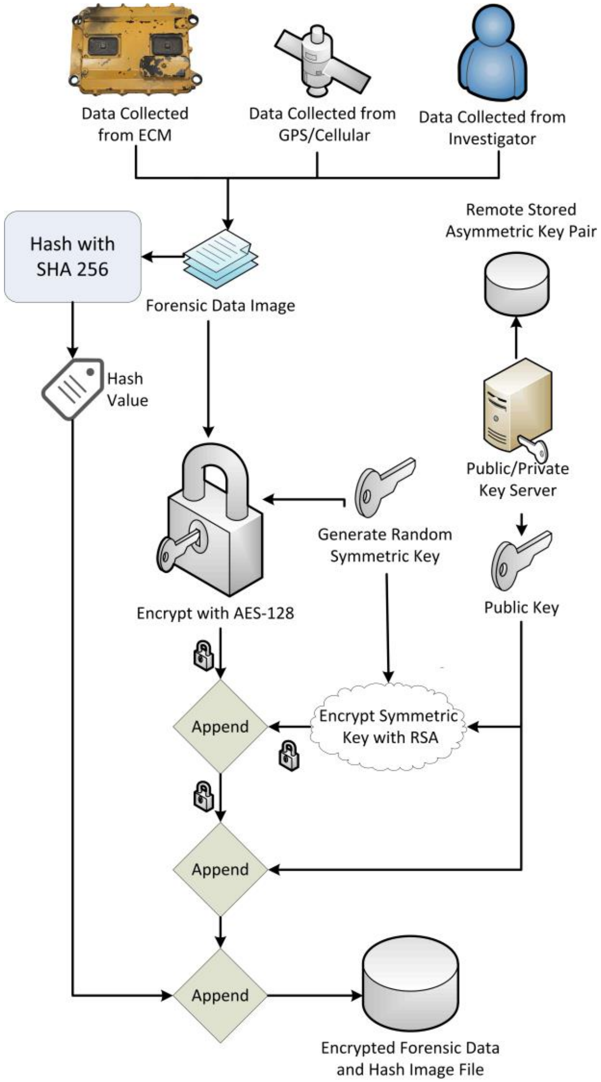
Prevent altering data.

Detect altered data or prove authentic data using SHA-256

Use 2 layer Cryptographic system

1. Symmetric AES-128
2. Asymmetric RSA-256

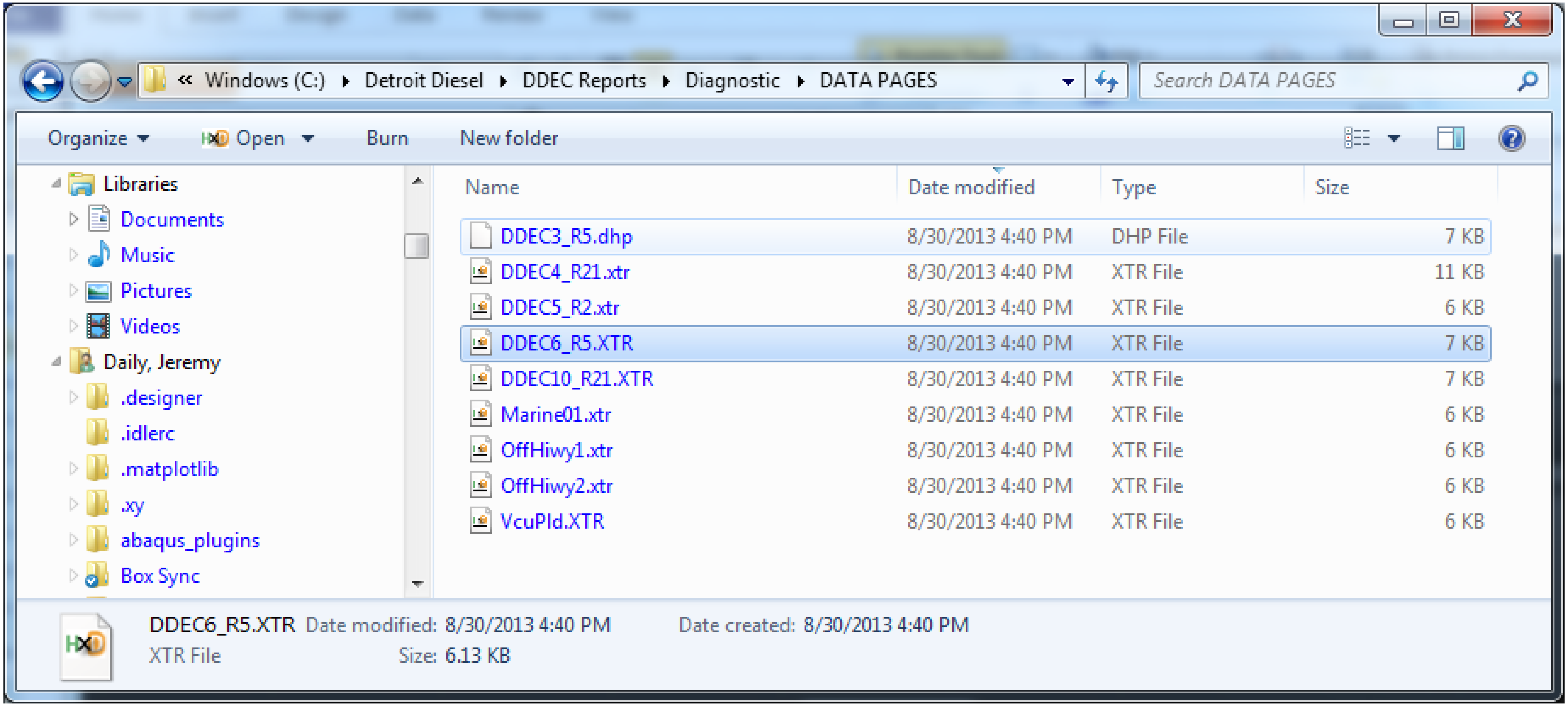
Open design with robust algorithms.


Data Collected from ECM
Data Collected from GPS/Cellular
Data Collected from Investigator
Remote Stored Asymmetric Key Pair
Hash with SHA 256
Forensic Data Image
Hash Value
Public/Private Key Server
Generate Random Symmetric Key
Encrypt with AES-128
Public Key
Append
Encrypt Symmetric Key with RSA
Append
Append
Encrypted Forensic Data and Hash Image File

Produce File Signatures

Immediate Recommendation: HashTab

Example: Find a DDEC Reports File, Right Click -> Properties



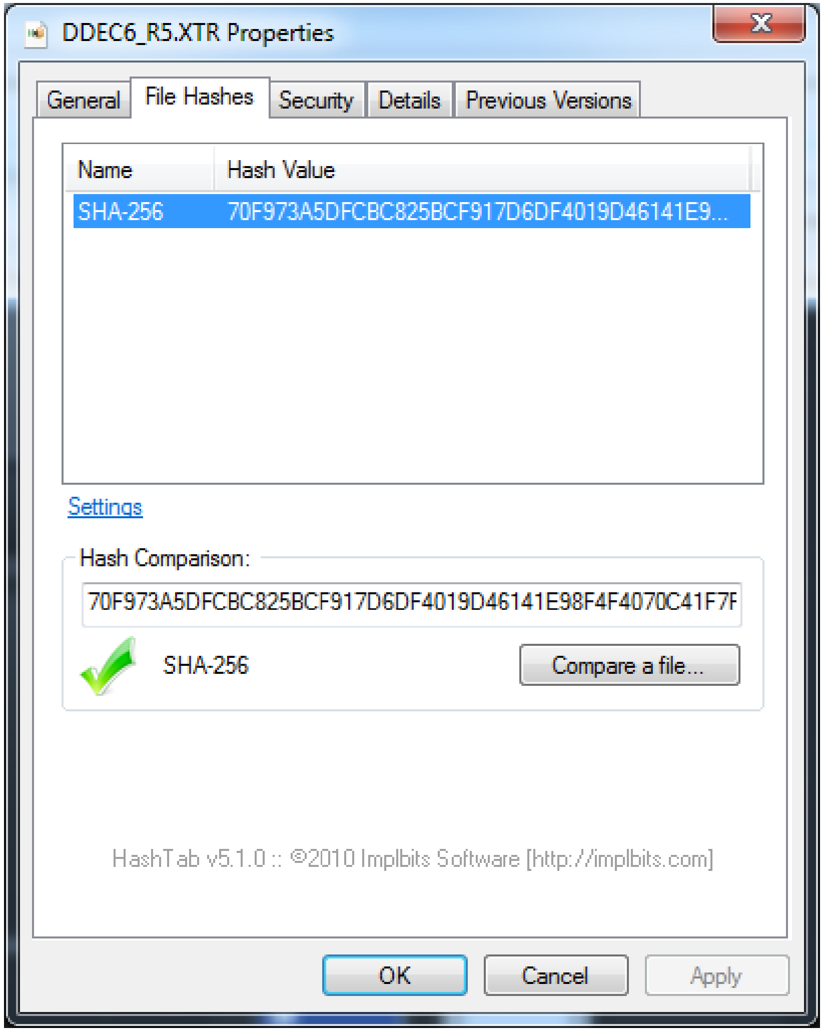
Name	Date modified	Type	Size
DDEC3_R5.dhp	8/30/2013 4:40 PM	DHP File	7 KB
DDEC4_R21.xtr	8/30/2013 4:40 PM	XTR File	11 KB
DDEC5_R2.xtr	8/30/2013 4:40 PM	XTR File	6 KB
DDEC6_R5.XTR	8/30/2013 4:40 PM	XTR File	7 KB
DDEC10_R21.XTR	8/30/2013 4:40 PM	XTR File	7 KB
Marine01.xtr	8/30/2013 4:40 PM	XTR File	6 KB
OffHiwy1.xtr	8/30/2013 4:40 PM	XTR File	6 KB
OffHiwy2.xtr	8/30/2013 4:40 PM	XTR File	6 KB
VcuPld.XTR	8/30/2013 4:40 PM	XTR File	6 KB

DDEC6_R5.XTR Date modified: 8/30/2013 4:40 PM Date created: 8/30/2013 4:40 PM
XTR File Size: 6.13 KB

Produce File Signatures (Cont.)

Windows Explorer Extension contains different hash algorithms

SHA-256 is sufficient.



DDEC6_R5.XTR Properties

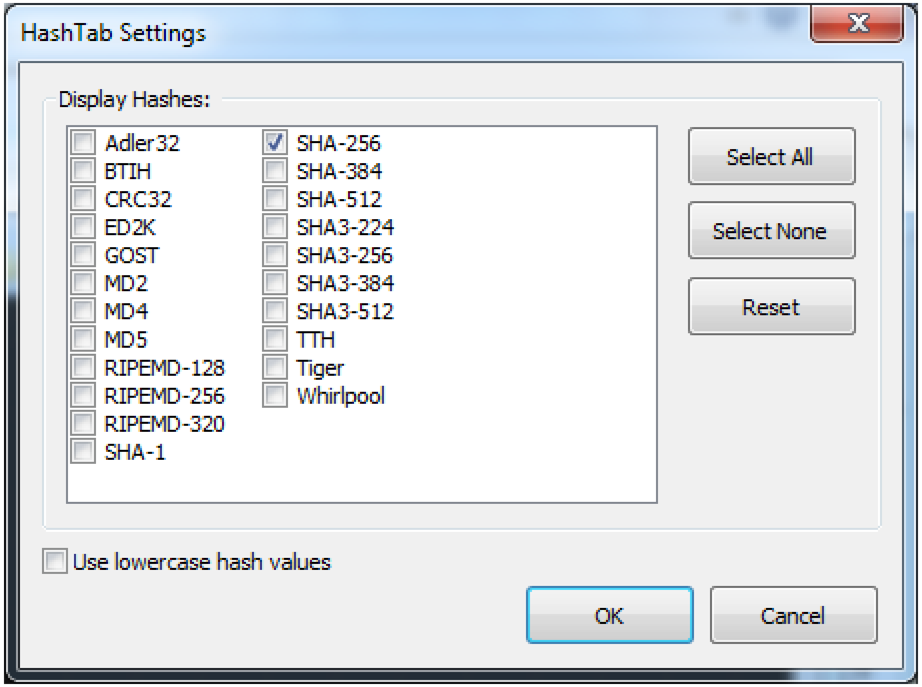
Name	Hash Value
SHA-256	70F973A5DFCBC825BCF917D6DF4019D46141E9...

Hash Comparison:

70F973A5DFCBC825BCF917D6DF4019D46141E98F4F4070C41F7F

✓ SHA-256

HashTab v5.1.0 :: ©2010 Implbits Software [http://implbits.com]



HashTab Settings

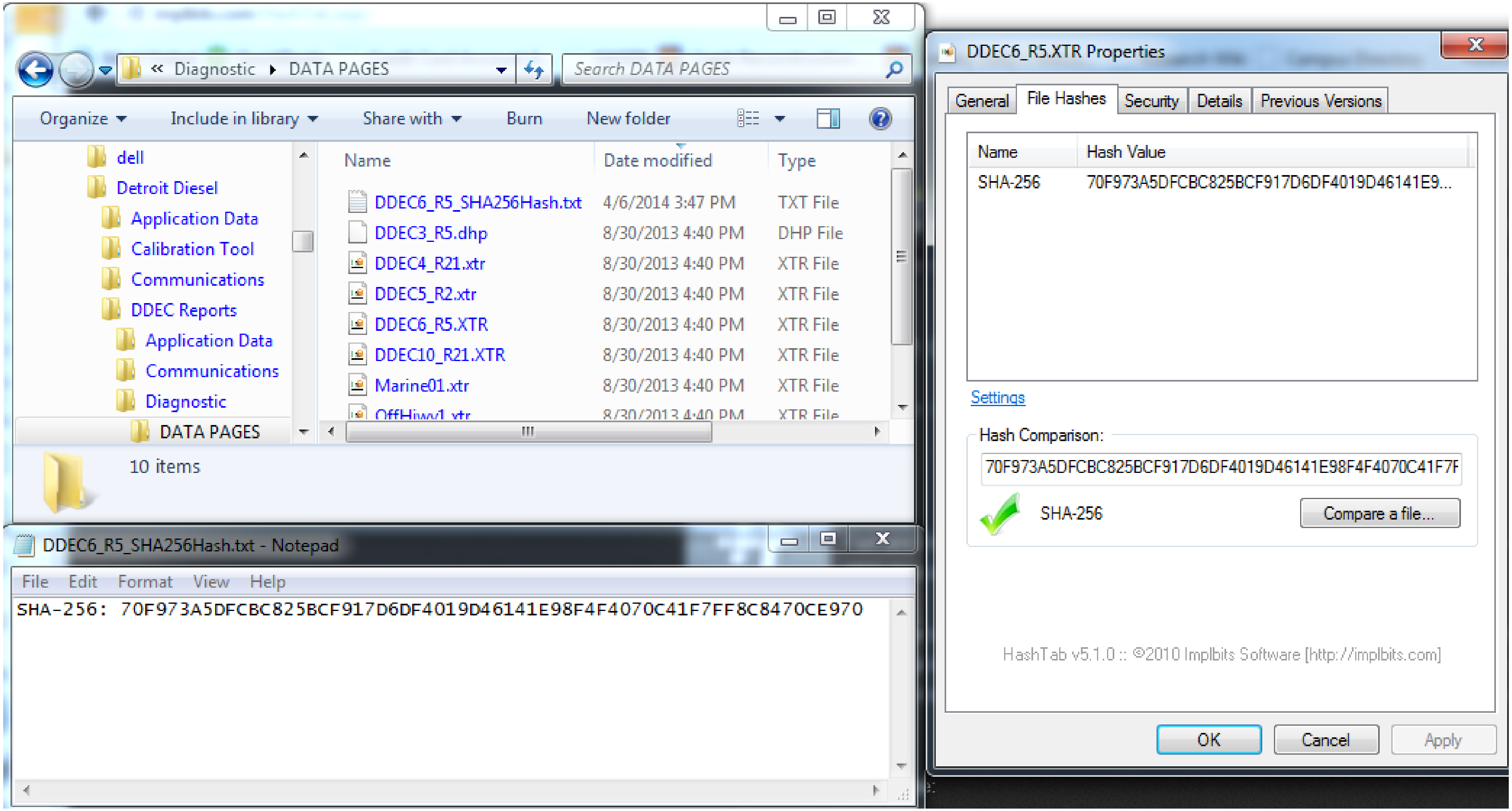
Display Hashes:

- □ Adler32
- □ BTIH
- □ CRC32
- □ ED2K
- □ GOST
- □ MD2
- □ MD4
- □ MD5
- □ RIPEMD-128
- □ RIPEMD-256
- □ RIPEMD-320
- □ SHA-1
- ☑ SHA-256
- □ SHA-384
- □ SHA-512
- □ SHA3-224
- □ SHA3-256
- □ SHA3-384
- □ SHA3-512
- □ TTH
- □ Tiger
- □ Whirlpool

□ Use lowercase hash values

Compute and Store the Hash Digest

Save Hash to a Text File.



Name	Date modified	Type
DDEC6_R5_SHA256Hash.txt	4/6/2014 3:47 PM	TXT File
DDEC3_R5.dhp	8/30/2013 4:40 PM	DHP File
DDEC4_R21.xtr	8/30/2013 4:40 PM	XTR File
DDEC5_R2.xtr	8/30/2013 4:40 PM	XTR File
DDEC6_R5.XTR	8/30/2013 4:40 PM	XTR File
DDEC10_R21.XTR	8/30/2013 4:40 PM	XTR File
Marine01.xtr	8/30/2013 4:40 PM	XTR File
OffHiwy1.xtr	8/30/2013 4:40 PM	XTR File

DDEC6_R5_SHA256Hash.txt - Notepad

```
SHA-256: 70F973A5DFCBC825BCF917D6DF4019D46141E98F4F4070C41F7FF8C8470CE970
```

DDEC6_R5.XTR Properties

Name	Hash Value
SHA-256	70F973A5DFCBC825BCF917D6DF4019D46141E9...

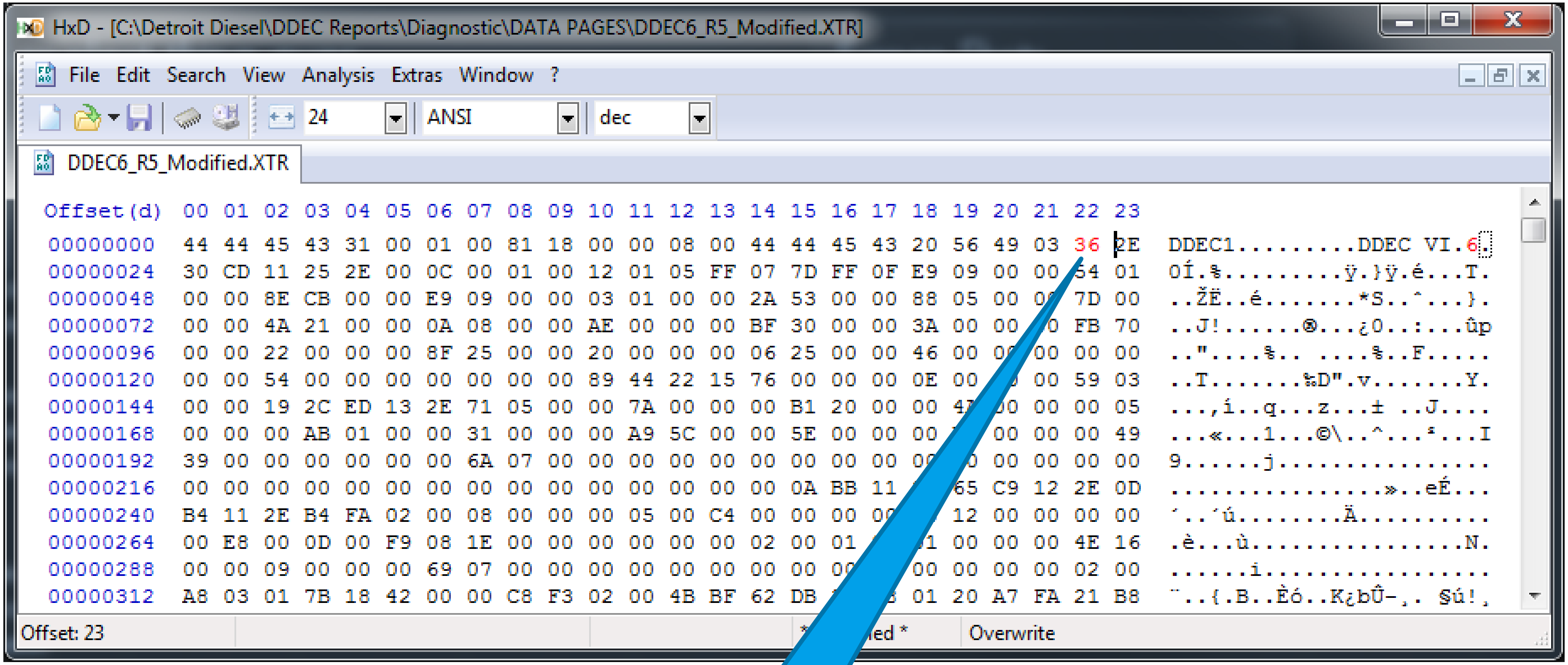
Hash Comparison:

70F973A5DFCBC825BCF917D6DF4019D46141E98F4F4070C41F7F

✓ SHA-256

HashTab v5.1.0 :: ©2010 Implbits Software [http://implbits.com]

Example: Alter a byte in the .XTR file



HxD - [C:\Detroit Diesel\DDEC Reports\Diagnostic\DATA PAGES\DDEC6_R5_Modified.XTR]

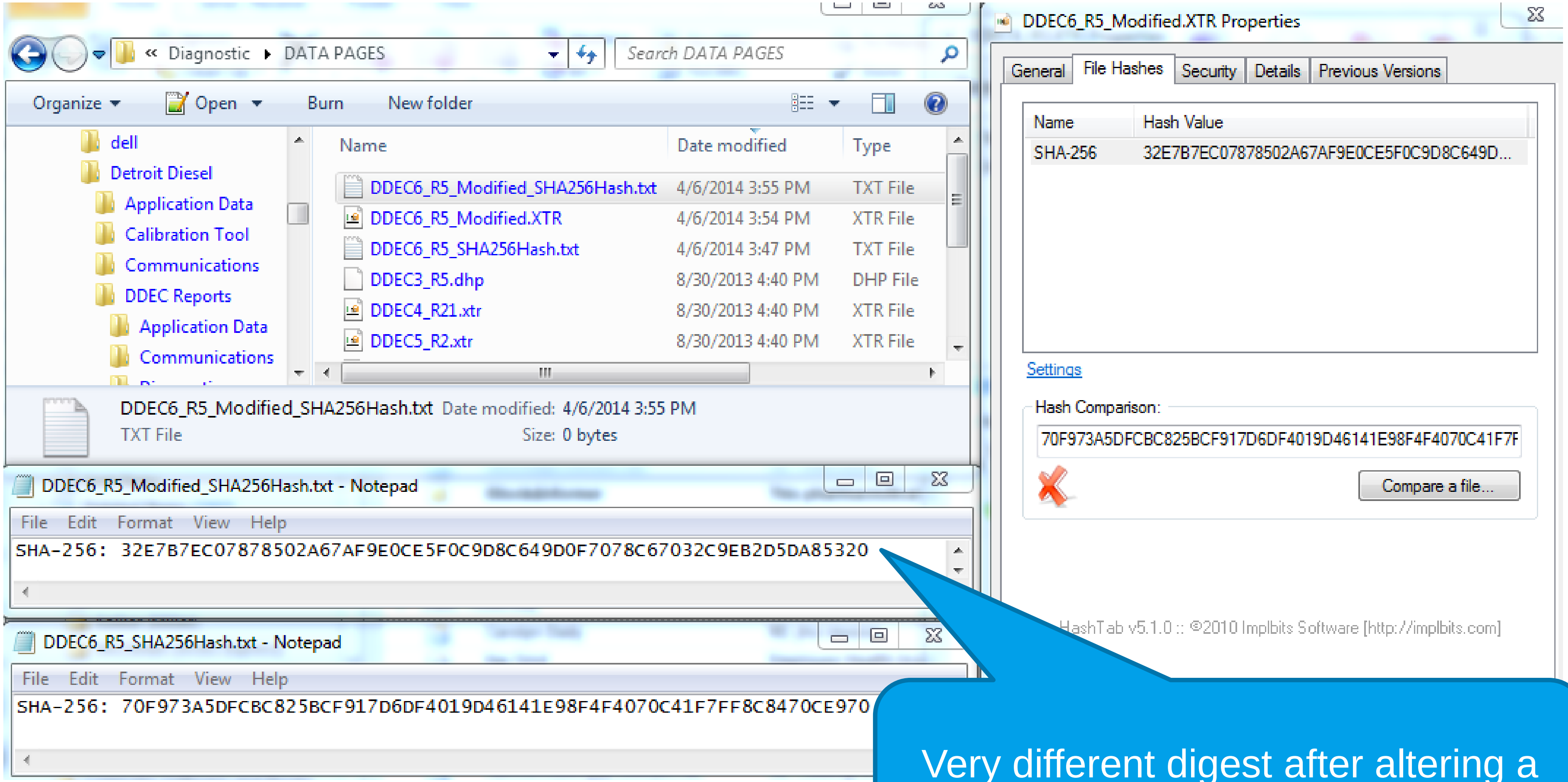
24 | ANSI | dec

```
Offset(d) 00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23

00000000  44 44 45 43 31 00 01 00 81 18 00 00 08 00 44 44 45 43 20 56 49 03 36 2E  DDEC1.........DDEC VI.6.
00000024  30 CD 11 25 2E 00 0C 00 01 00 12 01 05 FF 07 7D FF 0F E9 09 00 00 54 01  0Í.%.........ÿ.}ÿ.é...T.
00000048  00 00 8E CB 00 00 E9 09 00 00 03 01 00 00 2A 53 00 00 88 05 00 00 7D 00  ..ŽË..é.......*S..ˆ...}.
00000072  00 00 4A 21 00 00 0A 08 00 00 AE 00 00 00 BF 30 00 00 3A 00 00 00 FB 70  ..J!......®...¿0..:...ûp
00000096  00 00 22 00 00 00 8F 25 00 00 20 00 00 00 06 25 00 00 46 00 00 00 00 00  .."....%.. ....%..F.....
00000120  00 00 54 00 00 00 00 00 00 00 89 44 22 15 76 00 00 00 0E 00 00 00 59 03  ..T.......‰D".v.......Y.
00000144  00 00 19 2C ED 13 2E 71 05 00 00 7A 00 00 00 B1 20 00 00 4A 00 00 00 05  ...,í..q...z...± ..J....
00000168  00 00 00 AB 01 00 00 31 00 00 00 A9 5C 00 00 5E 00 00 00 AA 00 00 00 49  ...«...1...©\..^...ª...I
00000192  39 00 00 00 00 00 00 6A 07 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  9......j................
00000216  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0A BB 11 [illegible] 65 C9 12 2E 0D  ................»..eÉ...
00000240  B4 11 2E B4 FA 02 00 08 00 00 00 05 00 C4 00 00 00 00 [illegible] 12 00 00 00 00  ´..´ú........Ä..........
00000264  00 E8 00 0D 00 F9 08 1E 00 00 00 00 00 00 02 00 01 [illegible] [illegible] 00 00 00 4E 16  .è...ù................N.
00000288  00 00 09 00 00 00 69 07 00 00 00 00 00 00 00 00 00 [illegible] 00 00 00 00 02 00  ......i.................
00000312  A8 03 01 7B 18 42 00 00 C8 F3 02 00 4B BF 62 DB 96 82 01 20 A7 FA 21 B8  ¨..{.B..Èó..K¿bÛ–‚. §ú!¸
```

Offset: 23 | *[illegible]ied * | Overwrite

Change 35 to 36

Compare Hashes to Detect Alteration



Name	Date modified	Type
DDEC6_R5_Modified_SHA256Hash.txt	4/6/2014 3:55 PM	TXT File
DDEC6_R5_Modified.XTR	4/6/2014 3:54 PM	XTR File
DDEC6_R5_SHA256Hash.txt	4/6/2014 3:47 PM	TXT File
DDEC3_R5.dhp	8/30/2013 4:40 PM	DHP File
DDEC4_R21.xtr	8/30/2013 4:40 PM	XTR File
DDEC5_R2.xtr	8/30/2013 4:40 PM	XTR File

DDEC6_R5_Modified_SHA256Hash.txt Date modified: 4/6/2014 3:55 PM
TXT File Size: 0 bytes

DDEC6_R5_Modified_SHA256Hash.txt - Notepad

```
SHA-256: 32E7B7EC07878502A67AF9E0CE5F0C9D8C649D0F7078C67032C9EB2D5DA85320
```

DDEC6_R5_SHA256Hash.txt - Notepad

```
SHA-256: 70F973A5DFCBC825BCF917D6DF4019D46141E98F4F4070C41F7FF8C8470CE970
```

DDEC6_R5_Modified.XTR Properties

Name	Hash Value
SHA-256	32E7B7EC07878502A67AF9E0CE5F0C9D8C649D...

Hash Comparison: 70F973A5DFCBC825BCF917D6DF4019D46141E98F4F4070C41F7F

HashTab v5.1.0 :: ©2010 Implbits Software [http://implbits.com]

Very different digest after altering a couple bits. Alteration is detected.

Email digest to a trusted 3rd party.

Forensic Replay Mechanism

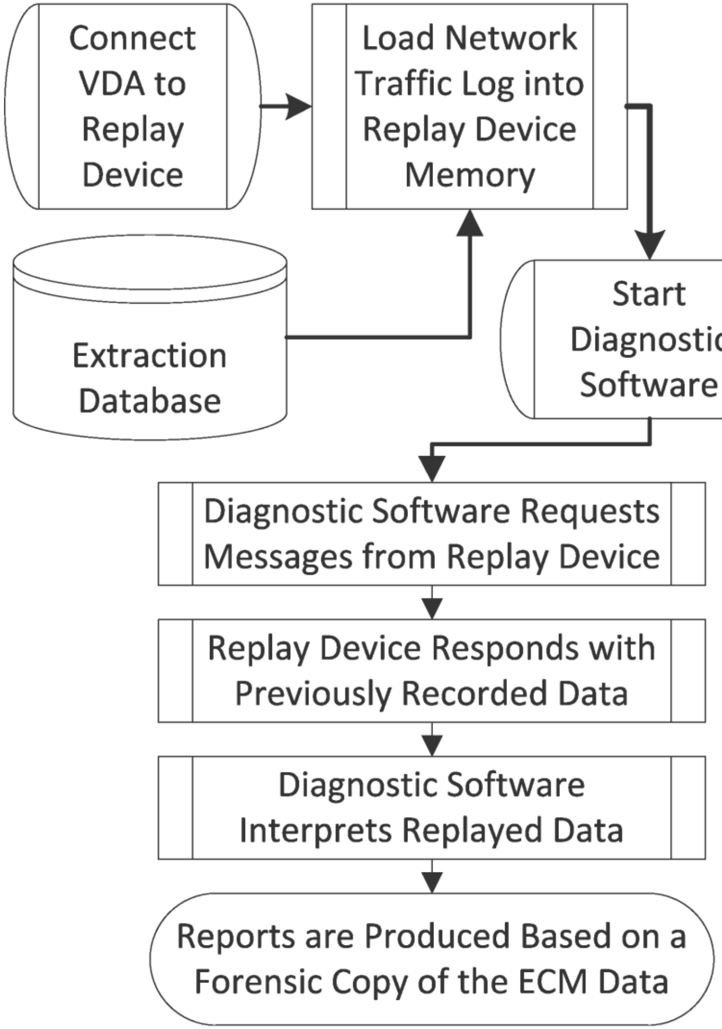
The network traffic can be a trusted source of data.

If network traffic is

- Captured,
- Hashed, and
- Stored,

then it represents a “forensic” image.

Example: Capturing forensically sound network traffic saves significant field time (no screenshots are needed).


Connect VDA to Replay Device
Load Network Traffic Log into Replay Device Memory
Extraction Database
Start Diagnostic Software
Diagnostic Software Requests Messages from Replay Device
Replay Device Responds with Previously Recorded Data
Diagnostic Software Interprets Replayed Data
Reports are Produced Based on a Forensic Copy of the ECM Data

Summary and Conclusion

Current software is not forensically sound.

Trust is established with experts. Sometimes authenticity cannot be established.

Some concepts were proposed to make HVEDR data forensically sound.

Presentation available at:

http://tucrrc.utulsa.edu/