LogView - Supportforum

Fragen rund um unsere Auswert-Software

Hacking - ELV 8x00 Lader

Autor	Nachricht
Dominik Site Admin  Anmeldungsdatum: 17.02.2005 Beiträge: 143 Wohnort: Madfeld	Verfasst am: So Apr 24, 2005 8:36 pm Titel: Hacking - ELV 8x00 Lader zitat

Moin !

Es gibt Hersteller die sträuben sich leider, dass Datenformat eines Laders preiszugeben. Nutzen tut es eigentlich eh nix, denn prinzipiell kann man Formate die über eine RS232 Schnittstelle gehen, sehr einfach mitschneiden und anschließend hacken oder sagen wir mal lieber entschlüsseln...

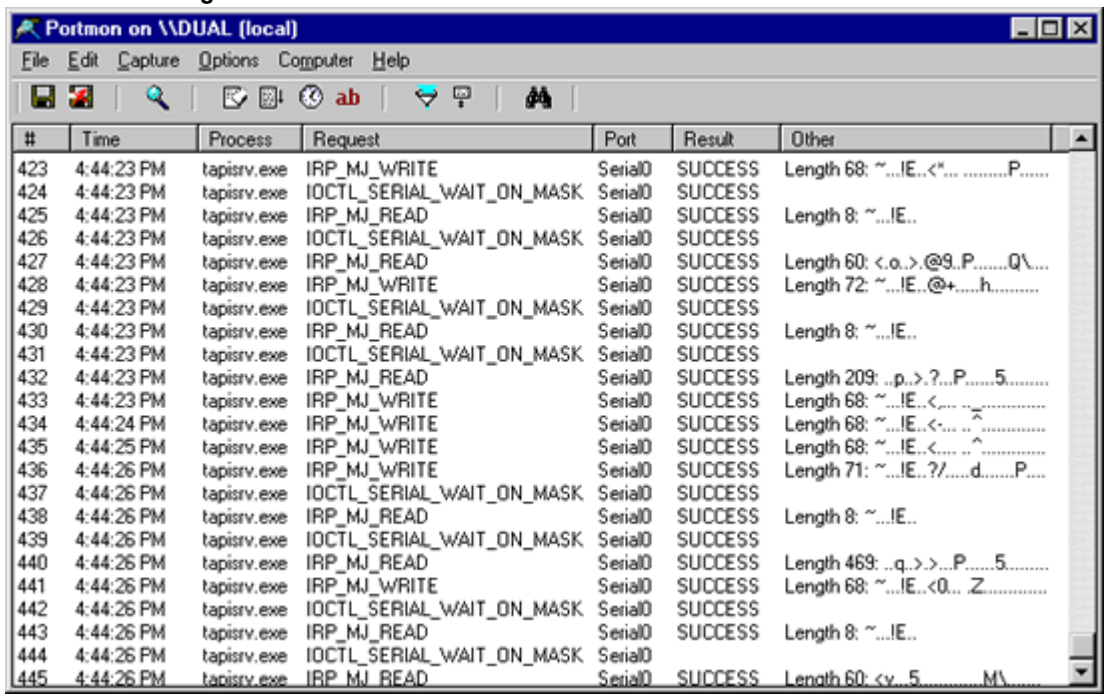
Teil I - Schnittstellenparameter finden

Um das Datenformat zu entschlüsseln müssen wir erstmal die Einstellungen der Schnittstelle rausfinden. Dazu muss man auch noch wissen, dass die ELV Lader nicht wirklich USB nutzen. Es ist vielmehr ein seriell <> USB Konverter eingebaut. Es wird also über einen USB Port eine serielle Schnittstelle simuliert. Das ändert aber nichts an der Tatsache, dass wir das mitschneiden können und das wir erstmal das Format finden müssen, als wie die Schnittstelle selber konfiguriert werden muss, um die Daten überhaupt sinnvoll zu erkennen.

Dazu machen wir dann mal folgendes:
Auf http://www.sysinternals.com/ gehen und PortMon runterladen
(http://www.sysinternals.com/ntw2k/freeware/portmon.shtml). Wenn du XP hast den für WinNT ganz unten runterladen. Dann

startest du das Teil und klickst unter "Computer" auf Connect Local. Unter Capture noch den richtigen Port anhaken wo der Lader angeschlossen ist.
Wenn bei den Ikons das dritte eine normale Lupe (ohne rotes X) ist, dann ist Portmon im Aufzeichnugsmodus. Starte jetzt mal die normale Anwendung von dem Lader und starte z.B. ganz normal eine Aufzeichnung (Es reicht vollkommen wenn du ca. 10 Sekunden was aufzeichnest!!). Dann kopier mal alles was im Portmon ist und pack es in diesen Fred (Dazu in Portmon die erste Zeile anklicken, nach ganz unten scrollen, STRG drücken und dann die letzte Zeile anklicken.)

Die Aufzeichnung sollte in etwa so aussehen:



#	Time	Process	Request	Port	Result	Other
423	4:44:23 PM	tapisrv.exe	IRP_MJ_WRITE	Serial0	SUCCESS	Length 68: ~...IE..<*... .....P.....
424	4:44:23 PM	tapisrv.exe	IOCTL_SERIAL_WAIT_ON_MASK	Serial0	SUCCESS	
425	4:44:23 PM	tapisrv.exe	IRP_MJ_READ	Serial0	SUCCESS	Length 8: ~...IE..
426	4:44:23 PM	tapisrv.exe	IOCTL_SERIAL_WAIT_ON_MASK	Serial0	SUCCESS	
427	4:44:23 PM	tapisrv.exe	IRP_MJ_READ	Serial0	SUCCESS	Length 60: <.o..>.@9..P.....Q\....
428	4:44:23 PM	tapisrv.exe	IRP_MJ_WRITE	Serial0	SUCCESS	Length 72: ~...IE..@+.....h.....
429	4:44:23 PM	tapisrv.exe	IOCTL_SERIAL_WAIT_ON_MASK	Serial0	SUCCESS	
430	4:44:23 PM	tapisrv.exe	IRP_MJ_READ	Serial0	SUCCESS	Length 8: ~...IE..
431	4:44:23 PM	tapisrv.exe	IOCTL_SERIAL_WAIT_ON_MASK	Serial0	SUCCESS	
432	4:44:23 PM	tapisrv.exe	IRP_MJ_READ	Serial0	SUCCESS	Length 209: ..p..>.?...P.....5.....
433	4:44:23 PM	tapisrv.exe	IRP_MJ_WRITE	Serial0	SUCCESS	Length 68: ~...IE..<,... ..^.....
434	4:44:24 PM	tapisrv.exe	IRP_MJ_WRITE	Serial0	SUCCESS	Length 68: ~...IE..<-... ..^.....
435	4:44:25 PM	tapisrv.exe	IRP_MJ_WRITE	Serial0	SUCCESS	Length 68: ~...IE..<.... ..^.....
436	4:44:26 PM	tapisrv.exe	IRP_MJ_WRITE	Serial0	SUCCESS	Length 71: ~...IE..?/.....d.....P....
437	4:44:26 PM	tapisrv.exe	IOCTL_SERIAL_WAIT_ON_MASK	Serial0	SUCCESS	
438	4:44:26 PM	tapisrv.exe	IRP_MJ_READ	Serial0	SUCCESS	Length 8: ~...IE..
439	4:44:26 PM	tapisrv.exe	IOCTL_SERIAL_WAIT_ON_MASK	Serial0	SUCCESS	
440	4:44:26 PM	tapisrv.exe	IRP_MJ_READ	Serial0	SUCCESS	Length 469: ..q..>.>...P.....5.....
441	4:44:26 PM	tapisrv.exe	IRP_MJ_WRITE	Serial0	SUCCESS	Length 68: ~...IE..<0... .Z.....
442	4:44:26 PM	tapisrv.exe	IOCTL_SERIAL_WAIT_ON_MASK	Serial0	SUCCESS	
443	4:44:26 PM	tapisrv.exe	IRP_MJ_READ	Serial0	SUCCESS	Length 8: ~...IE..
444	4:44:26 PM	tapisrv.exe	IOCTL_SERIAL_WAIT_ON_MASK	Serial0		
445	4:44:26 PM	tapisrv.exe	IRP_MJ_READ	Serial0	SUCCESS	Length 60: <v...5.....M\.....

Allerdings müsste oben was von Baudrate und Parität stehen. Das sieht dann in etwa so aus:
0 0.05700222 svchost.exe IRP_MJ_CREATE Serial2 SUCCESS Options: Open
1 0.00000363 svchost.exe IRP_MJ_CLEANUP Serial2 SUCCESS
2 0.00000419 svchost.exe IRP_MJ_DEVICE_CONTROL Serial2 INVALID PARAMETER IOCTL: 0x2B002C
3 0.00244891 svchost.exe IOCTL_SERIAL_SET_DTR Serial2 SUCCESS

4 0.00000168 svchost.exe IOCTL_SERIAL_SET_BAUD_RATE Serial2 SUCCESS
5 0.00000251 svchost.exe IOCTL_SERIAL_GET_PROPERTIES Serial2 SUCCESS
6 0.00000196 svchost.exe IOCTL_SERIAL_GET_BAUD_RATE Serial2 SUCCESS
7 0.00000196 svchost.exe IOCTL_SERIAL_GET_LINE_CONTROL Serial2 SUCCESS
8 0.00000140 svchost.exe IOCTL_SERIAL_GET_CHARS Serial2 SUCCESS
9 0.00000140 svchost.exe IOCTL_SERIAL_GET_HANDFLOW Serial2 SUCCESS
10 0.00341943 svchost.exe IOCTL_SERIAL_SET_BAUD_RATE Serial2 SUCCESS Rate: 19200
11 0.00295373 svchost.exe IOCTL_SERIAL_SET_DTR Serial2 SUCCESS
12 0.00719393 svchost.exe IOCTL_SERIAL_SET_LINE_CONTROL Serial2 SUCCESS StopBits: 1 Parity: NONE WordLength: 8
13 0.00000587 svchost.exe IOCTL_SERIAL_SET_CHAR Serial2 SUCCESS EOF:0 ERR:0 BRK:0 EVT:0 XON:11 XOFF:13
14 0.00267688 svchost.exe IOCTL_SERIAL_SET_HANDFLOW Serial2 SUCCESS Shake:9 Replace:80 XonLimit:10 XoffLimit:10
15 0.00000615 svchost.exe IOCTL_SERIAL_PURGE Serial2 SUCCESS Purge: TXABORT RXABORT
16 0.00000168 svchost.exe IOCTL_SERIAL_CLEAR_STATS Serial2 SUCCESS
17 0.00000168 svchost.exe IOCTL_SERIAL_PURGE Serial2 SUCCESS Purge: RXABORT
18 0.00000140 svchost.exe IOCTL_SERIAL_SET_TIMEOUTS Serial2 SUCCESS RI:20 RM:0 RC:0 WM:10 WC:2000
20 0.06132567 svchost.exe IRP_MJ_READ Serial2 CANCELLED Length 1

Hier steht alles nötige wie Baudrate, Parität, Datenbits, etc. drin. Genaugenommen sind folgende Zeilen für uns interessant:
... IOCTL_SERIAL_SET_BAUD_RATE Serial2 SUCCESS Rate: 19200
Liefert uns die Baudrate

... IOCTL_SERIAL_SET_LINE_CONTROL Serial2 SUCCESS StopBits: 1 Parity: NONE WordLength: 8
Liefert uns die Anzahl Datenbytes und die Anzahl StopBits, sowie die Art der Parität

... IOCTL_SERIAL_SET_CHAR Serial2 SUCCESS EOF:0 ERR:0 BRK:0 EVT:0 XON:11 XOFF:13
... IOCTL_SERIAL_SET_HANDFLOW Serial2 SUCCESS Shake:9 Replace:80 XonLimit:10 XoffLimit:10
liefert uns Infos über das Handshakeverfahren (sofern es überhaupt genutzt wird)

Wenn wir diese Daten haben, können wir über gehen zum Teil II - dem eigentlichen Aufzeichnen von Daten.

Teil II - Aufzeichnen von Daten

Jetzt wird es heikel, aber wer es bis hier geschafft hat, der sollte auch mit dem Folgenden fertig werden
Bei diesen Ladern stellen sich grundsätzlich erstmal zwei unterschiedliche Probleme:
1) der Lader empfängt

Es ist ja kein Geheimnis, dass der Lader auch Daten vom PC annehmen kann. Wenn ich das richtig verstehe, dann kann man den Lader quasi komplett vom PC aus konfigurieren. Wir müssen uns also was einfallen lassen wie wir an diese Daten kommen, die an den Lader gesendet werden. Das geht nur über einen Web, ein Serieller Sniffer wie PortMon. Die Verwendung habe ich ja schon etwas weiter oben beschrieben.
Wir starten also Portmon und dann die Anwendung des Laders. Dort stellen wir nun z.B. ein Ladeprogramm (ich kenne die Settings leider nicht genau) ein und sagen der Software > Übertragen zum Lader. Nun zeichnet ja Portmon im Hintergrund die Daten mit auf. Also haben wir ja die Infos die wir wollen. ABER: Bitte notiert euch zu den Daten, was ihr da genau gemacht habt, also was ihr in der Software eingestellt habt. Wenn man das nicht weiss, dann nutzen die Infos meist recht wenig.
Es macht auch durchaus Sinn, verschiedene Konfigurationen an den Lader zu senden (am besten jede die er kann ...). So kann man die Unterschiede besser feststellen.
Also immer schon die Daten des Portmon in eine Textdatei kopieren und dazuschreiben was ihr da eingestellt habt.

2) der Lader sendet
Der Lader wird ja seine Infos während dem Laden (und evtl. auch permanent) an den PC senden. Diese Daten können wir natürlich auch mit dem PortMon protokollieren. Aber das ist etwas umständlich. Hier ist es besser, die Daten mit dem SerialWatcher aufzuzeichnen. Was ihr dazu zu tun habt steht hier beschrieben: http://www.logview.info/?Specials:Daten_aufzeichnen
WICHTIG: Bitte stellt den SerialWatcher richtig ein. Wenn der falsch konfiguriert ist (z.B. falsche Baudrate), dann zeichnet ihr nur Müll auf!!!
Am besten erstmal die Ergebnisse von Teil I hier posten und dann schauen wir mal weiter.

Soderle, das ist eine Menge Holz was ich hier geschrieben habe und ich wette es kann auch nicht jeder umsetzten aber wir schaffen das schon

Nachtrag:
Ich habe eben doch schon was rausgefunden ... Habe da mal ne Mail bekommen. Also der Lader hat schonmal folgende Schnittstellenparameter: '38400,e,8,1,p'
Bedeutet: 38400 Baud, Parität EVEN, 8 Datenbits, 1 Stopbit. Aber evtl. kann das ja mal einer verifizieren.

Soderle, ich hoffe mal auf Mithilfe
_____
Greetz Dominik (Webadmin)
Skype: schmidom
ICQ: 22210387

Nach oben

profil pn email www ICQ-Nummer

XNeo

Verfasst am: Mo Apr 25, 2005 11:22 pm Titel:

zitat

Anmeldungsdatum: 25.04.2005
Beiträge: 1

Servus!

Danke für die Einführung, aber ich glaube, die brauch' ich nicht .

Porteinstellungen scheinen bei mir 9600/8/N/1 ohne Flußsteuerung zu sein (das sagt zumindest der USB2Serial-Treiber (FTDI)).

Ich benutze seit einigen Tagen die Shareware von Serial Monitor. Damit "belausche" ich die Charge-Professional Software. Beim Starten wird ja erstmal die Akku-Datenbank aus dem Gerät geholt, deswegen habe ich damit angefangen.

Was ich bisher weiß:

Code:

```
================================================================================
ELV 8500-2 Steuercodes (bekannt)
================================================================================

--------------------------------------------------------------------------------
Generelles
--------------------------------------------------------------------------------

Der Lader sendet nichts von alleine, sondern beantwortet lediglich Anfragen
vom PC.

Nachrichtenbeginn: 02
Nachrichtenende  : 03

Escape-Zeichen   : 05
Escape-Sequenzen : 02 => 05 12
                 : 03 => 05 13
                 : 05 => 05 15

Beim Beginn jeder Antwort wird die Anfrage (der Befehl) wiederholt.

--------------------------------------------------------------------------------
Abfrage Gerätedaten
--------------------------------------------------------------------------------
Anfrage: 02 75 03
```

```
Antwort: 02 75
         ** ** ** **    <--\
         ** ** ** **    <-- 9 ASCII-Zeichen, Firmware
         **             <--/
         FF FF
         ** ** ** **    <--\
         ** ** ** **    <-- 10 ASCII-Zeichen, Seriennummer
         ** **          <--/
         03

--------------------------------------------------------------------------------
Abfrage Akku-Datenbank
--------------------------------------------------------------------------------
Anfrage: 02 64 ## 03    <-- ## = 00 bis 27, Nummern der 40 Speicherplätze

Antwort: 02 64 ##
         ** ** ** **    <--\
         ** ** ** **    <-- 9 ASCII-Zeichen, Name des Akkus; ggf.
         **             <--/        mit Leerzeichen aufgefüllt
         xx             <-- xx = 00 für NiCd, 01 für NiMH, 05 12 für Li-Ion,
                                    05 13 für Li-Pol, 04 für Pb,
                                    FF für "nicht belegt"
         yy             <-- yy = Zellenzahl
         02 62 5A 00    <-- Kapazität in 1/10.000mAh (hier: 40000000*1/10000mAh)
         1F 40          <-- Entladestrom in 1/10mA (hier: 8000*1/10mA)
         0F A0          <-- Ladestrom in 1/10mA (hier: 4000*1/10mA)
         01 2C          <-- Wartezeit C/D in Sekunden (hier: 300 Sekunden)
         00             <-- Activator (für Bleiakkus)? (00 = aus; 01 = ein)
         03

--------------------------------------------------------------------------------
Abfrage Temperaturen
--------------------------------------------------------------------------------
Anfrage: 02 74 03

Antwort: 02 74
         AB E0          <-- Temperatur Kanal 1 (Sensor) in 1/100°C oder
                            (wie hier) "AB E0" für "Kein Sensor angeschlossen"
         0A BF          <-- Temperatur Trafo in 1/100°C (Hier: 2751 * 1/100°C)
         09 89          <-- Temperatur Kühlkörper in 1/100°C
                            (Hier: 2441 * 1/100°C)
         03
```

Was ich noch nicht weiß:

Code:

```
================================================================================
ELV 8500-2 Steuercodes (unbekannt)
================================================================================

--------------------------------------------------------------------------------
Abfrage ?a (Kanalabhängig)
--------------------------------------------------------------------------------
Anfrage: 02 6D ## 03    <-- ## = Kanalnummer; 00, 01, 05 12 oder 05 13

Antwort: 02 6D ##
         00 00 00 00
         00 00 00 00
         03

--------------------------------------------------------------------------------
Abfrage ?b (Kanalabhängig)
--------------------------------------------------------------------------------
Anfrage: 02 61 ## 03    <-- ## = Kanalnummer; 00, 01, 05 12 oder 05 13

Antwort: 02 61 ##
         00
         03


--------------------------------------------------------------------------------
Abfrage ?c (Kanalabhängig)
--------------------------------------------------------------------------------
Anfrage: 02 70 ## 03    <-- ## = Kanalnummer; 00, 01, 05 12 oder 05 13

Antwort: 02 70 ##
         00 01 06 17
         70 27 10 01
         C9 C3 80 05    <-- Achtung, 05 12 = 02 (Escaping)
         12 05 15 78    <-- Achtung, 05 15 = 05 (Escaping)
         05 13 84 00    <-- Achtung, 05 13 = 03 (Escaping)
         00 00
         03

--------------------------------------------------------------------------------
Abfrage ?d
--------------------------------------------------------------------------------
Anfrage: 02 67 03       <--

Antwort: 02 67
         05 13 84 05    <-- Achtung, 05 13 = 03 (Escaping)
         13 E8 0B B8
         0C 1C 07 08
         0A 0A 0A 0A
```

```
05 15 05 15    <-- Achtung, 05 15 = 05 (Escaping)
05 15 05 15    <-- Achtung, 05 15 = 05 (Escaping)
05 15 28 14    <-- Achtung, 05 15 = 05 (Escaping)
03
```

Ablaufübersicht:

Code:

```
================================================================================
Ablauf beim Starten von ChargeProfessional (nur Anfragen vom PC)
================================================================================
02 75 03                <-- Gerätedaten

02 64 00 03             <-- Abfrage Akku-DB, Satz #1
02 64 01                <-- Abfrage Akku-DB, Satz #2
02 64 05 12 03          <-- Abfrage Akku-DB, Satz #3
02 64 05 13 03          <-- Abfrage Akku-DB, Satz #4
02 64 04 03             <-- Abfrage Akku-DB, Satz #5
02 64 05 15 03          <-- Abfrage Akku-DB, Satz #6
02 64 06 03             <-- Abfrage Akku-DB, Satz #7
02 64 07 03             <-- Abfrage Akku-DB, Satz #8
02 64 08 03             <-- Abfrage Akku-DB, Satz #9
[...]                   <-- [...]
02 64 27 03             <-- Abfrage Akku-DB, Satz #40

02 70 00 03             <-- Abfrage ?c Kanal 1
02 70 01 03             <-- Abfrage ?c Kanal 2
02 70 05 12 03          <-- Abfrage ?c Kanal 3
02 70 05 13 03          <-- Abfrage ?c Kanal 4

02 67 03                <-- ?d

02 70 00 03             <-- Abfrage ?c Kanal 1
02 70 01 03             <-- Abfrage ?c Kanal 2
02 70 05 12 03          <-- Abfrage ?c Kanal 3
02 70 05 13 03          <-- Abfrage ?c Kanal 4

02 74 03                <-- Abfrage Temperaturen
02 6D 00 03             <-- Abfrage ?a Kanal 1
02 6D 01 03             <-- Abfrage ?a Kanal 2
02 6D 05 12 03          <-- Abfrage ?a Kanal 3
02 6D 05 13 03          <-- Abfrage ?a Kanal 4
02 61 00 03             <-- Abfrage ?b Kanal 1
02 61 01 03             <-- Abfrage ?b Kanal 2
02 61 05 12 03          <-- Abfrage ?b Kanal 3
```

```
02 61 05 13 03          <-- Abfrage ?b Kanal 4
02 70 00 03             <-- Abfrage ?c Kanal 1
02 70 01 03             <-- Abfrage ?c Kanal 2
02 70 05 12 03          <-- Abfrage ?c Kanal 3
02 70 05 13 03          <-- Abfrage ?c Kanal 4

Danach alle 5 Sekunden (beginn jedoch sofort):
02 74 03                <-- Abfrage Temperaturen
02 6D 00 03             <-- Abfrage ?a Kanal 1
02 6D 01 03             <-- Abfrage ?a Kanal 2
02 6D 05 12 03          <-- Abfrage ?a Kanal 3
02 6D 05 13 03          <-- Abfrage ?a Kanal 4
02 61 00 03             <-- Abfrage ?b Kanal 1
02 61 01 03             <-- Abfrage ?b Kanal 2
02 61 05 12 03          <-- Abfrage ?b Kanal 3
02 61 05 13 03          <-- Abfrage ?b Kanal 4
02 70 00 03             <-- Abfrage ?c Kanal 1
02 70 01 03             <-- Abfrage ?c Kanal 2
02 70 05 12 03          <-- Abfrage ?c Kanal 3
02 70 05 13 03          <-- Abfrage ?c Kanal 4
```

Ich editiere dieses Posting, wenn ich mehr 'rausbekomme.

Gruß,

_____

Henning.

_____

PHP - People Hate Perl

Nach oben profil pn

Beiträge der letzten Zeit anzeigen: Alle Beiträge | Die ältesten zuerst | Los

neuesthema antwort erstellen LogView - Supportforum Foren-Übersicht -> Ladegeräte

Alle Zeiten sind GMT + 1 Stunde

Seite 1 von 1

Gehe zu: Ladegeräte | Los

Du kannst Beiträge in dieses Forum schreiben.
Du kannst auf Beiträge in diesem Forum antworten.

Du kannst deine Beiträge in diesem Forum nicht bearbeiten.
Du kannst deine Beiträge in diesem Forum nicht löschen.
Du kannst an Umfragen in diesem Forum nicht mitmachen.
Du kannst Dateien in diesem Forum posten
Du kannst Dateien in diesem Forum herunterladen