Crimson 3.0 DSP/HMI/MC/PTV Digital Signatures for Data Log Validation

Digital Signature of Log Files

This document describes the method used by Red Lion Controls operator panels to apply digital signatures to log files so as to ensure and verify their integrity. The method is published to allow third parties to satisfy themselves as to the security of the algorithm, and to write their own verification software should they wish to have independent confirmation of the integrity of a given file. The source code of Red Lion's command-line verifier is similarly available for inspection, and for use as the basis of other verification tools.

LOG FILE STRUCTURE

Each log file comprises a header line, and a number of data lines. Each line in the file is terminated with a CR-LF sequence. The header line comprises comma-separated labels for the data fields in the file. Each data line comprises time and date information, followed by comma-separated data fields appropriate to the log file in question. The data fields are followed by a comma, and then a signature block, which starts with a two-digit hexadecimal type code. The type code is followed by a dash, and then an eight-digit hexadecimal sequence number. The sequence number increases monotonically. It is based on a non-resetable counter stored within the non-volatile memory of the G3. A given sequence number will never be used more than once, making it impossible for a G3 to produce the same output line twice, even if the real-time clock is wound-back. The sequence number is followed by a dash, and then a further six-digit hexadecimal number equal to the least significant portion of the operator panel's Ethernet MAC identifier. This field allows a file to be traced to a given device, as the identifiers are allocated during manufacture so that each unit has a unique assignment. If the type code is 00, no further data is included. If the type code is 01, the MAC identifier is followed by another dash, and a 256-digit hexadecimal number containing a digital signature. The last line of a valid log file will always be a type-01 signature block. A type-01 block will occur at least every 32768 bytes in the data. Type-01 signature blocks may occur on consecutive lines.

SIGNATURE GENERATION

The 256-digit hexadecimal number is an RSA digital signature based upon the MD5 hash of certain bytes in the file. For the first type-01 block in a given file, the byte stream begins with the first byte of the file i.e. the first character of the header line. For subsequent type-01 blocks, the stream starts with the '0' at the start of the prior type-01 block. The stream comprises all characters from this first character, to the last character of the line to which the signature block is to be appended. This last line excludes any CR-LF sequence, as this has yet to be output, and similarly excludes the signature block itself or the separating comma. Any prior lines include their CR-LF sequences. The MD5 hash of this stream is then taken, and the 1024-bit RSA digital signature is then computed using a key pair with the following public key…

```
-----BEGIN PUBLIC KEY BLOCK----
mQCPA0J44BAAAAEEAMWLFSXQZtP6cEto4diYLOj9QTafi2ZHv+9FEfi3S+jqA+7T
xvpxXNYbiEk4hzA9+C7JE6vy+pnwJdgxKyRG304+IyTlx1OEMll4m8kR2OYiBoZf
w1o53YUZPBCWAK0ENvmOl0Wex7mZ5W3uVA7tktu0nhP05u8tEr5IzTi+HuhzABEB
AAG0C3JlZGxpb24ubmV0iQCVAwUQQnjgEL5IzTi+HuhzAQENewP/bUmq9JVgPgbZ
qRJ+UfC8+aSGy6hplCUl/maTu4tU9mWWv5lPDZA+H56slbFVPidaeEZEN+WlFnWA
1fEfTrXI6CgUyKJ4egTuOAOn6MoV3VyZNS0lcP3xYW8arqTYX2ZTDbhZGYEGoyXz
64ti4VRWgKcGJrKd3c6/c2wxUrPSMSg=
=lnN8
-----END PUBLIC KEY BLOCK-----
```

The resulting signature is output in Little Endian order as a 256-digit hexadecimal number.

Security Features

The algorithm described above can detect the following kinds of tampering or misrepresentation:

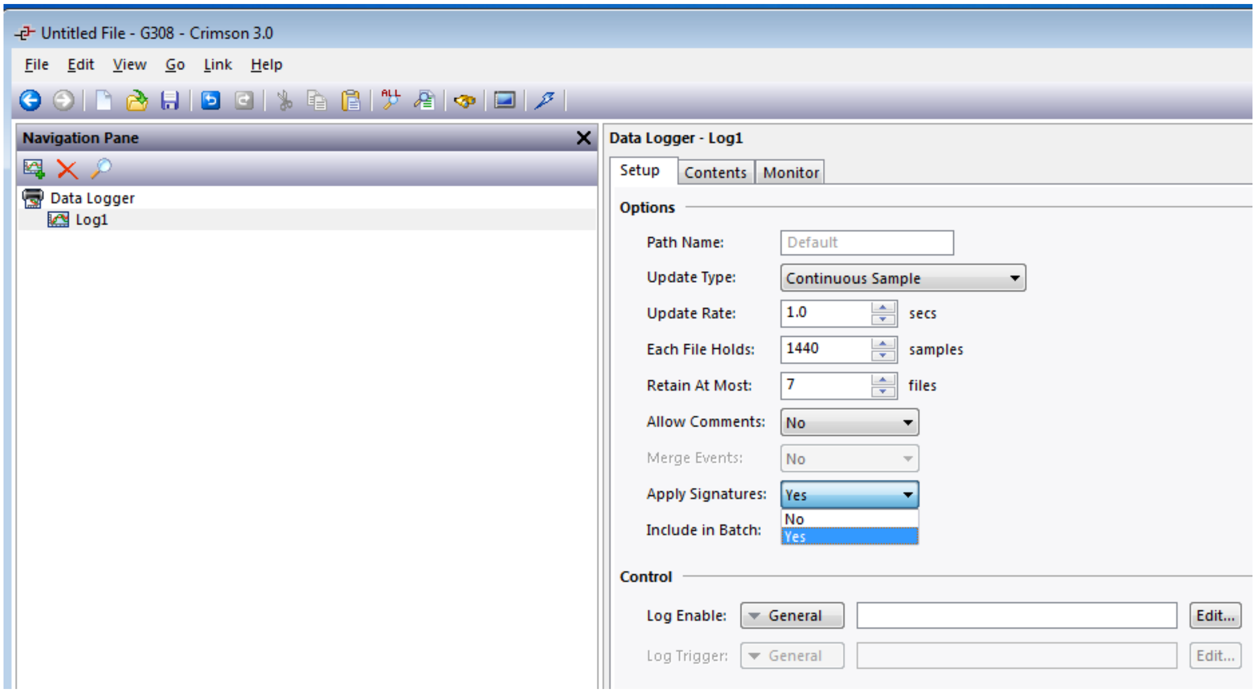
- Representation that the file came from a different G3 than the unit that actually produced it
- Attempts to recreate data within a sequence of files by re-winding the clock of an operator panel
- Changes to the data fields contained within the file or the header line thereto
- Re-ordering of lines (or blocks or lines) within the file
- Deletion of lines from the start or the middle of the file.

The algorithm cannot detect the deletion of lines at the end of a file if such deletion occurs, it will leave a valid type-01 signature block on its last line. This ability is not considered vital, as the absence of such data at the end of a file cannot in any case be taken as probative of any condition.

Enabling the Signatures

Crimson 3.0

1. Click on the log to validate.
2. Set Apply Signatures to *Yes*
3. Save and Download the file.



Path Name: Default

Update Type: Continuous Sample

Update Rate: 1.0 secs

Each File Holds: 1440 samples

Retain At Most: 7 files

Allow Comments: No

Merge Events: No

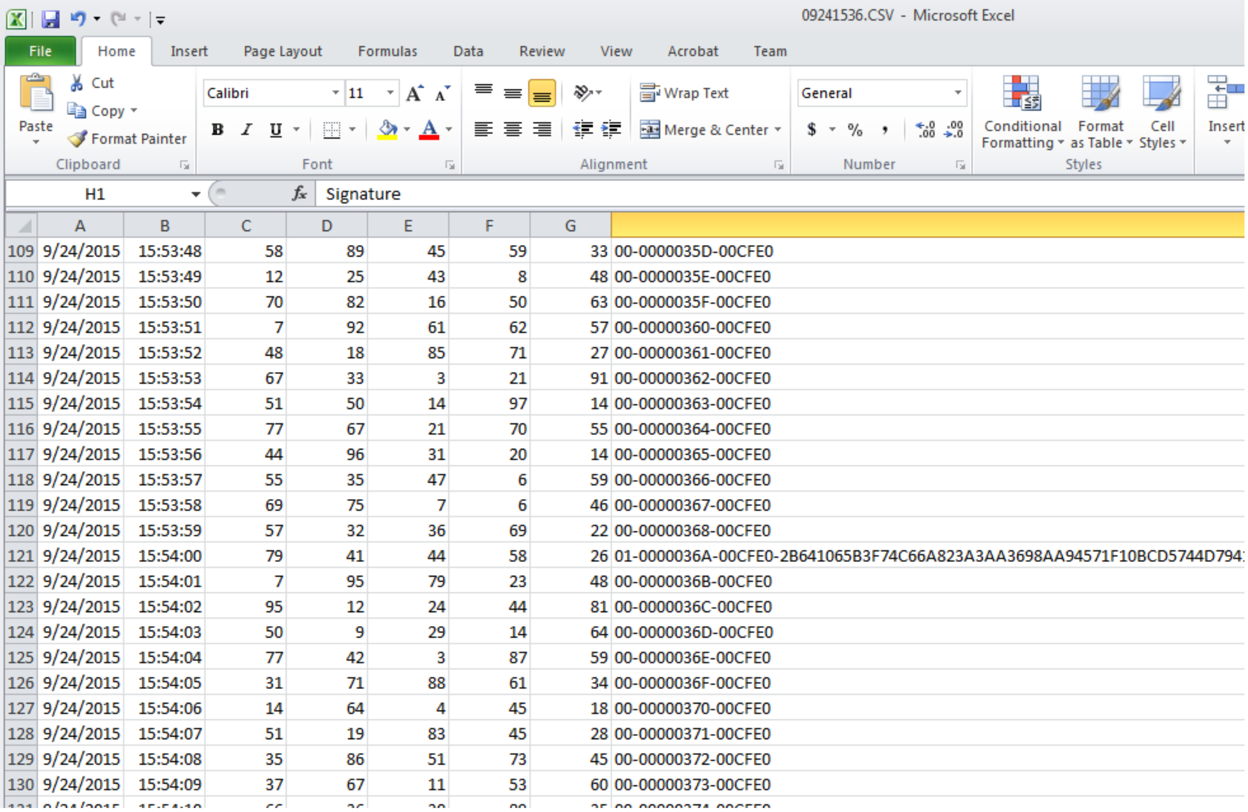
Apply Signatures: Yes (No / Yes)

Include in Batch:

Log Enable: General

Log Trigger: General

4. The resulting file will look something like this:



H1 *fx* Signature

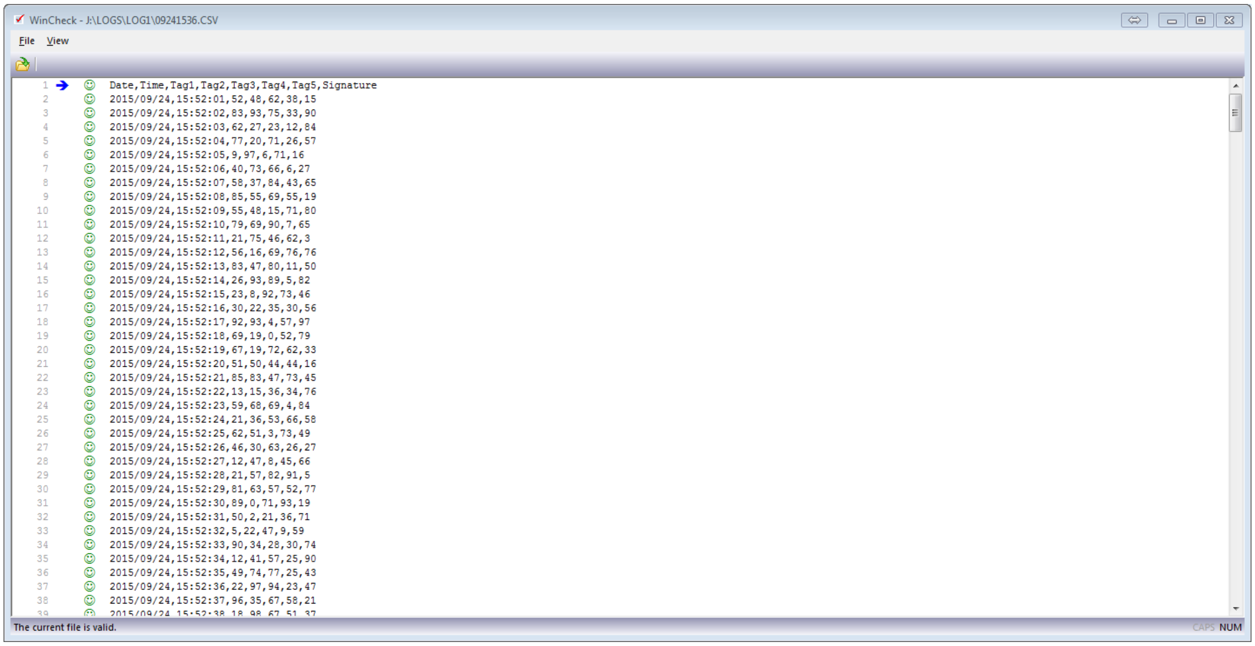
	A	B	C	D	E	F	G	
109	9/24/2015	15:53:48	58	89	45	59	33	00-0000035D-00CFE0
110	9/24/2015	15:53:49	12	25	43	8	48	00-0000035E-00CFE0
111	9/24/2015	15:53:50	70	82	16	50	63	00-0000035F-00CFE0
112	9/24/2015	15:53:51	7	92	61	62	57	00-00000360-00CFE0
113	9/24/2015	15:53:52	48	18	85	71	27	00-00000361-00CFE0
114	9/24/2015	15:53:53	67	33	3	21	91	00-00000362-00CFE0
115	9/24/2015	15:53:54	51	50	14	97	14	00-00000363-00CFE0
116	9/24/2015	15:53:55	77	67	21	70	55	00-00000364-00CFE0
117	9/24/2015	15:53:56	44	96	31	20	14	00-00000365-00CFE0
118	9/24/2015	15:53:57	55	35	47	6	59	00-00000366-00CFE0
119	9/24/2015	15:53:58	69	75	7	6	46	00-00000367-00CFE0
120	9/24/2015	15:53:59	57	32	36	69	22	00-00000368-00CFE0
121	9/24/2015	15:54:00	79	41	44	58	26	01-0000036A-00CFE0-2B641065B3F74C66A823A3AA3698AA94571F10BCD5744D794
122	9/24/2015	15:54:01	7	95	79	23	48	00-0000036B-00CFE0
123	9/24/2015	15:54:02	95	12	24	44	81	00-0000036C-00CFE0
124	9/24/2015	15:54:03	50	9	29	14	64	00-0000036D-00CFE0
125	9/24/2015	15:54:04	77	42	3	87	59	00-0000036E-00CFE0
126	9/24/2015	15:54:05	31	71	88	61	34	00-0000036F-00CFE0
127	9/24/2015	15:54:06	14	64	4	45	18	00-00000370-00CFE0
128	9/24/2015	15:54:07	51	19	83	45	28	00-00000371-00CFE0
129	9/24/2015	15:54:08	35	86	51	73	45	00-00000372-00CFE0
130	9/24/2015	15:54:09	37	67	11	53	60	00-00000373-00CFE0

Validating File Data

Wincheck.exe

1. Run wincheck.exe from the Crimson 3.0 folder.
2. Select *Open* and choose the file to validate.
3. Click the *Open* button to view the results.

   a. Valid file, notice the green ☺

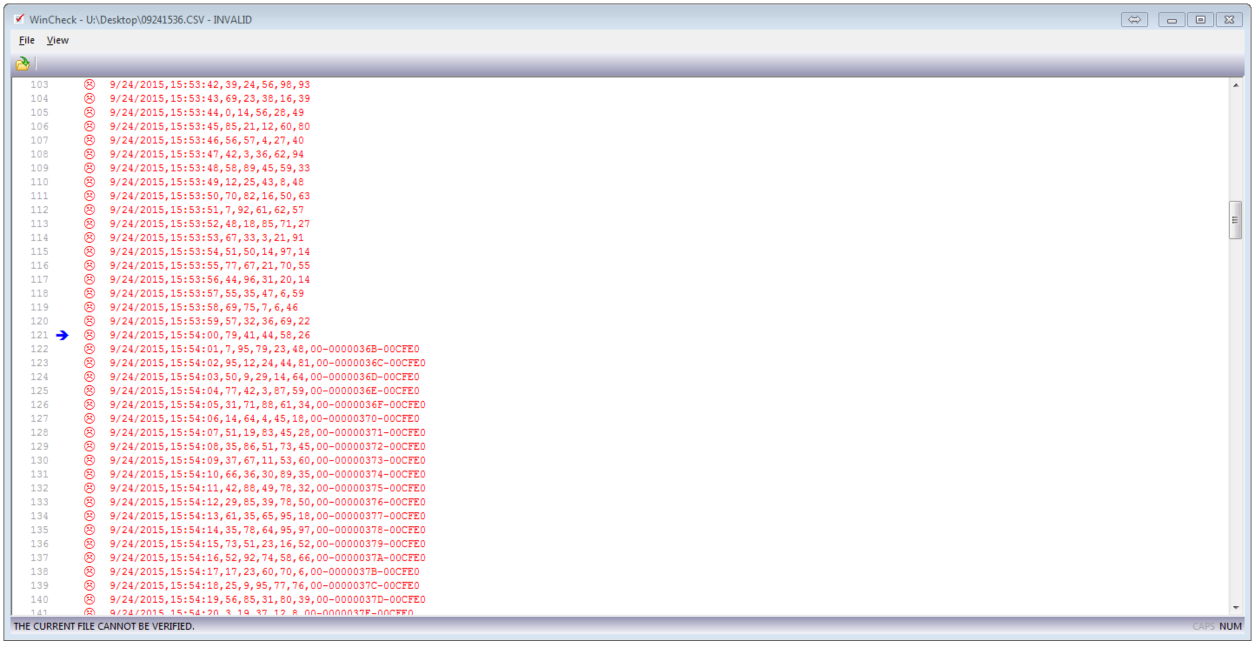


WinCheck - J:\LOGS\LOG1\09241536.CSV

```
☺ Date,Time,Tag1,Tag2,Tag3,Tag4,Tag5,Signature
☺ 2015/09/24,15:52:01,52,48,62,38,15
☺ 2015/09/24,15:52:02,83,93,75,33,90
☺ 2015/09/24,15:52:03,62,27,23,12,84
☺ 2015/09/24,15:52:04,77,20,71,26,57
☺ 2015/09/24,15:52:05,9,97,6,71,16
☺ 2015/09/24,15:52:06,40,73,66,6,27
☺ 2015/09/24,15:52:07,58,37,84,43,65
☺ 2015/09/24,15:52:08,85,55,69,55,19
☺ 2015/09/24,15:52:09,55,48,15,71,80
☺ 2015/09/24,15:52:10,79,69,90,7,65
☺ 2015/09/24,15:52:11,21,75,46,62,3
☺ 2015/09/24,15:52:12,56,16,69,76,76
☺ 2015/09/24,15:52:13,83,47,80,11,50
☺ 2015/09/24,15:52:14,26,93,89,5,82
☺ 2015/09/24,15:52:15,23,8,92,73,46
☺ 2015/09/24,15:52:16,30,22,35,30,56
☺ 2015/09/24,15:52:17,92,93,4,57,97
☺ 2015/09/24,15:52:18,69,19,0,52,79
☺ 2015/09/24,15:52:19,67,19,72,62,33
☺ 2015/09/24,15:52:20,51,50,44,44,16
☺ 2015/09/24,15:52:21,85,83,47,73,45
☺ 2015/09/24,15:52:22,13,15,36,34,76
☺ 2015/09/24,15:52:23,59,68,69,4,84
☺ 2015/09/24,15:52:24,21,36,53,66,58
☺ 2015/09/24,15:52:25,62,51,3,73,49
☺ 2015/09/24,15:52:26,46,30,63,26,27
☺ 2015/09/24,15:52:27,12,47,8,45,66
☺ 2015/09/24,15:52:28,21,57,82,91,5
☺ 2015/09/24,15:52:29,81,63,57,52,77
☺ 2015/09/24,15:52:30,89,0,71,93,19
☺ 2015/09/24,15:52:31,50,2,21,36,71
☺ 2015/09/24,15:52:32,5,22,47,9,59
☺ 2015/09/24,15:52:33,90,34,28,30,74
☺ 2015/09/24,15:52:34,12,41,57,25,90
☺ 2015/09/24,15:52:35,49,74,77,25,43
☺ 2015/09/24,15:52:36,22,97,94,23,47
☺ 2015/09/24,15:52:37,96,35,67,58,21
☺ 2015/09/24,15:52:38,18,98,67,51,37
```

The current file is valid.

   b. Invalid file, notice the red ☹



WinCheck - U:\Desktop\09241536.CSV - INVALID

```
☹ 9/24/2015,15:53:42,39,24,56,98,93
☹ 9/24/2015,15:53:43,69,23,38,16,39
☹ 9/24/2015,15:53:44,0,14,56,28,49
☹ 9/24/2015,15:53:45,85,21,12,60,80
☹ 9/24/2015,15:53:46,56,57,4,27,40
☹ 9/24/2015,15:53:47,42,3,36,62,94
☹ 9/24/2015,15:53:48,58,89,45,59,33
☹ 9/24/2015,15:53:49,12,25,43,8,48
☹ 9/24/2015,15:53:50,70,82,16,50,63
☹ 9/24/2015,15:53:51,7,92,61,62,57
☹ 9/24/2015,15:53:52,48,18,85,71,27
☹ 9/24/2015,15:53:53,67,33,3,21,91
☹ 9/24/2015,15:53:54,51,50,14,97,14
☹ 9/24/2015,15:53:55,77,67,21,70,55
☹ 9/24/2015,15:53:56,44,96,31,20,14
☹ 9/24/2015,15:53:57,55,35,47,6,59
☹ 9/24/2015,15:53:58,69,75,7,6,46
☹ 9/24/2015,15:53:59,57,32,36,69,22
☹ 9/24/2015,15:54:00,79,41,44,58,26
☹ 9/24/2015,15:54:01,7,95,79,23,48,00-0000036B-00CFE0
☹ 9/24/2015,15:54:02,95,12,24,44,81,00-0000036C-00CFE0
☹ 9/24/2015,15:54:03,50,9,29,14,64,00-0000036D-00CFE0
☹ 9/24/2015,15:54:04,77,42,3,87,59,00-0000036E-00CFE0
☹ 9/24/2015,15:54:05,31,71,88,61,34,00-0000036F-00CFE0
☹ 9/24/2015,15:54:06,14,64,4,45,18,00-00000370-00CFE0
☹ 9/24/2015,15:54:07,51,19,83,45,28,00-00000371-00CFE0
☹ 9/24/2015,15:54:08,35,86,51,73,45,00-00000372-00CFE0
☹ 9/24/2015,15:54:09,37,67,11,53,60,00-00000373-00CFE0
☹ 9/24/2015,15:54:10,66,36,30,89,35,00-00000374-00CFE0
☹ 9/24/2015,15:54:11,42,88,49,78,32,00-00000375-00CFE0
☹ 9/24/2015,15:54:12,29,85,39,78,50,00-00000376-00CFE0
☹ 9/24/2015,15:54:13,61,35,65,95,18,00-00000377-00CFE0
☹ 9/24/2015,15:54:14,35,78,64,95,97,00-00000378-00CFE0
☹ 9/24/2015,15:54:15,73,51,23,16,52,00-00000379-00CFE0
☹ 9/24/2015,15:54:16,52,92,74,58,66,00-0000037A-00CFE0
☹ 9/24/2015,15:54:17,17,23,60,70,6,00-0000037B-00CFE0
☹ 9/24/2015,15:54:18,25,9,95,77,76,00-0000037C-00CFE0
☹ 9/24/2015,15:54:19,56,85,31,80,39,00-0000037D-00CFE0
☹ 9/24/2015,15:54:20,3,19,37,12,8,00-0000037E-00CFE0
```

THE CURRENT FILE CANNOT BE VERIFIED.

Note: The signatures are shown once the data is unable to be validated. In this case the sample from 15:54:46 was removed, so the data from the previous save (15:54:00) onward cannot be validated.

Red Lion Technical Support

If you have any questions or trouble contact Red Lion Technical Support by emailing support@redlion.net or calling 1-877-432-9908.