Illegal WinCross Detection

Chris Morton

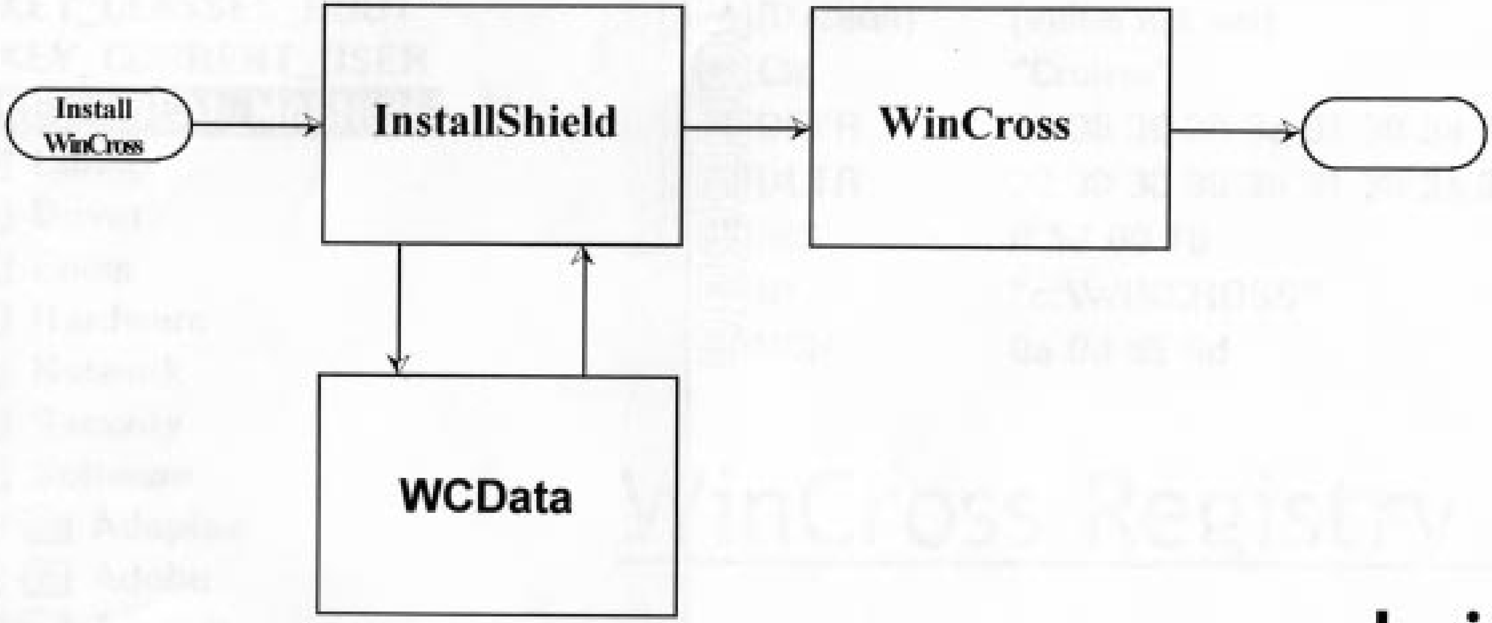
11/10/00

Initial WinCross Data Collection

1) Upon intial access, WINCROSS.EXE stores *encoded* date WinCross was first run (**DFTR**) in system Registry database.

2) Every launch thereafter, WINCROSS.EXE stores *encoded* date WinCross was last run (**DLTR**) in system Registry database.

IP is picked off during InstallShield



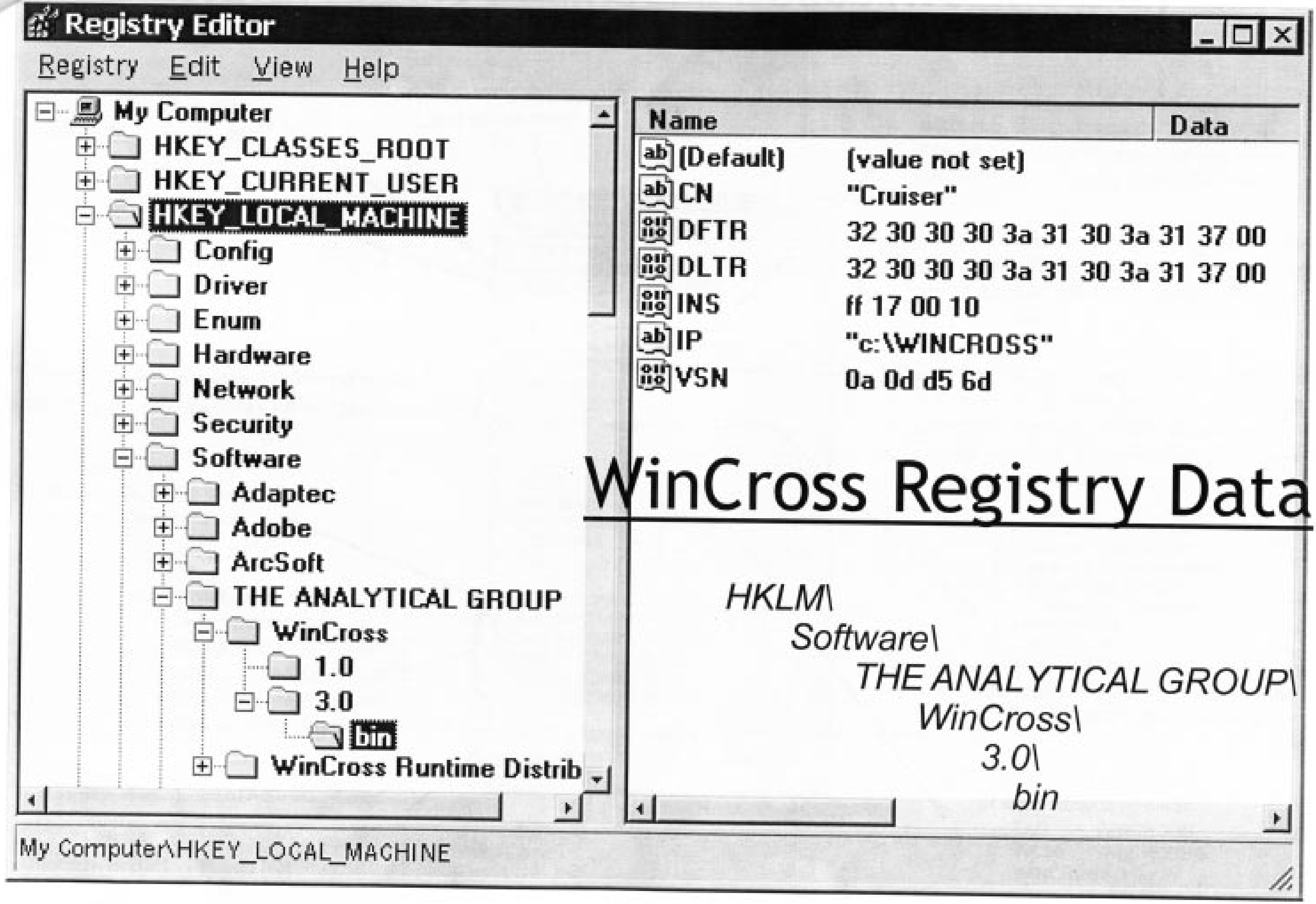
1) Detects volume serial number (**VSN**) in which WinCross is to be installed; stores *encoded* value in system Registry database.

2) Detects unique computer name (**CN**) of PC in which WinCross is to be installed; stores value in system Registry database.

3) Gets current date from computer during installation; stores as *encoded* (**INS**) value in system Registry database.

Note: **VSN**, **CN** , **INS** values *not* available for detection in initial versions of WinCross 3.0. However, such systems may be retrofitted to include **VSN** and **CN** values.

WinCross Registry Data



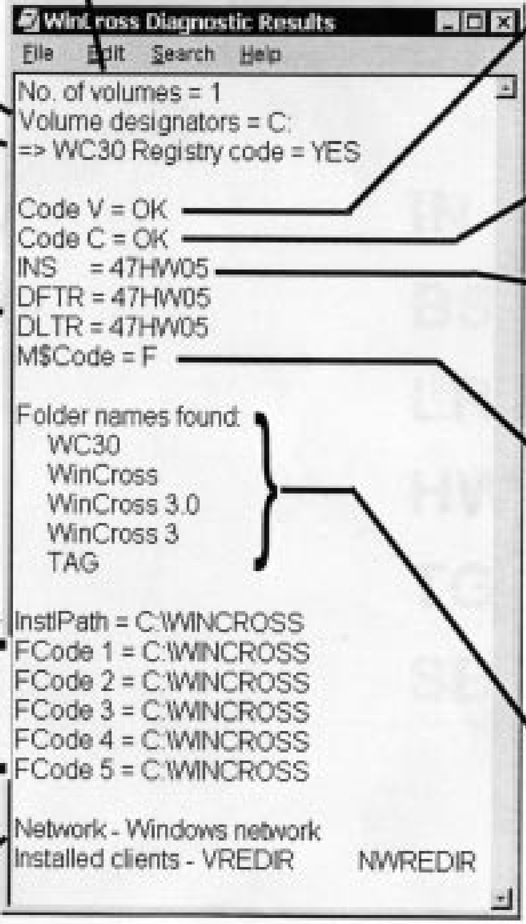
```
My Computer
  HKEY_CLASSES_ROOT
  HKEY_CURRENT_USER
  HKEY_LOCAL_MACHINE
    Config
    Driver
    Enum
    Hardware
    Network
    Security
    Software
      Adaptec
      Adobe
      ArcSoft
      THE ANALYTICAL GROUP
        WinCross
          1.0
          3.0
            bin
        WinCross Runtime Distrib
```

Name	Data
(Default)	(value not set)
CN	"Cruiser"
DFTR	32 30 30 30 3a 31 30 3a 31 37 00
DLTR	32 30 30 30 3a 31 30 3a 31 37 00
INS	ff 17 00 10
IP	"c:\WINCROSS"
VSN	0a 0d d5 6d

My Computer\HKEY_LOCAL_MACHINE

HKLM
Software
THE ANALYTICAL GROUP
WinCross
3.0
bin

WinCross 3.0 Diagnostic Codes (WCDIAG.EXE)



```
No. of volumes = 1
Volume designators = C:
=> WC30 Registry code = YES

Code V = OK
Code C = OK
INS    = 47HW05
DFTR = 47HW05
DLTR = 47HW05
M$Code = F

Folder names found:
    WC30
    WinCross
    WinCross 3.0
    WinCross 3
    TAG
InstlPath = C:\WINCROSS
FCode 1 = C:\WINCROSS
FCode 2 = C:\WINCROSS
FCode 3 = C:\WINCROSS
FCode 4 = C:\WINCROSS
FCode 5 = C:\WINCROSS

Network - Windows network
Installed clients - VREDIR          NWREDIR
```

1) How many drive partitions (volumes) does the user system have?

2) What are the drive volume designations (C:, D:, etc.)?

3) Has WinCross 3.0 ever been installed to this PC?

4) If there is a drive volume serial number mismatch, this code reports "**Code V = !!! ERROR !!!**". The only reason for this is the user is trying to illegally copy WinCross.

5) If there is a machine (PC) name mismatch, this code reports "**Code C = !!! ERROR !!!**". The only reason for this is the user is trying to illegally copy WinCross.

6) **INS** is the date WinCross 3.0 was installed on PC.
Day = Subtract **30** from the first number pair.
Month = See page four for month codes.
Year = Subtract **5** from the last number pair.

7) **DFTR** is the date WinCross 3.0 ***first ran*** on this PC:

8) **DLTR** is the date WinCross 3.0 ***last ran*** on this PC.

9) Operating system code:
A = Windows 2000 Server
B = Windows 2000 Professional
C = Windows NT Server
D = Windows NT Workstation
E = Windows Me
F = Windows 98
G = Windows 95

Also reports *Service Pack* number for Windows 2000/NT, if any installed.

10) Search and report existence of these folders, by name:
· TAG · WINCROSS
· WC30 · WINCROSS 3
· WINCROSS 3.0

11) What is the folder path to which WinCross was installed?

12) File locations:
FCode 1 = WINCROSS.41S
FCode 2 = WINCROSS.ENT
FCode 3 = WINCROSS.KEY
FCode 4 = WINCROSS.RST
FCode 5 = WINCROSS.EXE

13) Report existence of network, if any:

VREDIR - Microsoft network client installed
NWREDIR - Novell NetWare network client installed (can indicate Novell server on premises)