

3788/4
66
(11 fogli)
PROCURA DELLA REPUBBLICA
di Perugia
DEPOSITATO IN SEGRETARIA
24 APR 2008
M. SEGRETARIO

**Alla PROCURA DELLA REPUBBLICA
PRESSO IL TRIBUNALE DI PERUGIA**
(dr. G. MIGNINI)

INDICE

§ 1 – PREMESSA	pag. 03
§ 2 – QUESITO.....	pag. 04
§ 3 – ESAME DEL DISPOSITIVO	pag. 05
§ 4 – ATTIVITA' SVOLTA E RISULTATI CONSEGUITI.....	pag. 07
§ 5 –...CONCLUSIONI.....	pag. 09

§ 1 - PREMESSA

In data 9 aprile 2008, codesta A.G. ha conferito al sottoscritto I.C. Mario GATTONE del Servizio di Polizia Postale e delle Comunicazioni, l'incarico di eseguire gli accertamenti tecnici nell'ambito del procedimento penale n. 9066/07 sullo strumento "Logicube Desktop Write Protect" Serial # 51153 matr. USTG 0059 - 1942 "Fast-block" (dispositivo elettronico che si impiega nelle procedure di acquisizione forense) utilizzato dal Compartimento della Polizia Postale di Perugia per l'acquisizione dei dati contenuti negli hard disk Hitachi e Fujitsu appartenenti, rispettivamente, a Raffaele SOLLECITO e alla vittima KERCHER Meredith.

In data 17 aprile u.s. il Compartimento della Polizia Postale di Perugia ha consegnato allo scrivente la suindicata apparecchiatura che, il seguente 21 aprile, è stata sottoposta ad accertamento tecnico.

§ 2 – QUESITO

verificare l'integrità fisica e il corretto funzionamento del “Logicube Desktop Write Protect” Serial # 51153 matr. USTG 0059 - 1942 “Fast-block”

§ 3 – ESAME DEL DISPOSITIVO

SPECIFICHE DEL DISPOSITIVO



FIG.1

Il dispositivo Write-Protect™ (FIG 1) è stato creato per svolgere accertamenti forensi su supporti informatici di tipo hard disk, allorquando deve essere eseguita l'acquisizione e l'analisi dei dischi rigidi sotto stretto controllo, per evitare la "contaminazione" del disco oggetto della perizia.

L'adattatore è in grado di proteggere i dischi rigidi IDE dalle alterazioni (sia di natura dolosa che colposa), sia attraverso il collegamento diretto via cavo, o attraverso una connessione USB, come di seguito descritto. Il dispositivo è concepito per consentire al drive protetto solo sottoinsiemi ridotti dei comandi (comandi di lettura) conformi alle specifiche ATA e bloccare tutti gli altri comandi.

Il dispositivo Write-Protect™ può essere utilizzato in modi diversi. In particolare:

1. per proteggere un drive collegato direttamente ad una scheda madre, allo scopo di eseguire analisi investigative;
2. per proteggere un disco rigido sorgente durante un'acquisizione forense con dispositivi "Logicube Solitaire", "Solitaire Forensic", ecc.;
3. per proteggere un drive che risiede all'interno di un dispositivo "Logicube SF 5000u" quando è esaminato per mezzo di un PC attraverso una porta USB;
4. per consentire un collegamento di un drive autonomo ad un PC attraverso la porta USB e assicurare contestualmente la protezione del contenuto dello stesso drive.

Rilevazione dello stato iniziale del Logicube Desktop Write Protect" Serial # 51153 matr. USTG 0059 - 1942 "Fast-block" esaminato.

Lo strumento si presenta integro nelle parti elettroniche, meccaniche ed elettriche. Si accerta preliminarmente, mediante un tester, che le caratteristiche di tensione d'uscita del predetto dispositivo sono conformi ai valori previsti dalle specifiche tecniche standard degli hard disk con interfaccia ATA.

Lo strumento è custodito nell'apposita scatola originale provvisto di protezione anti-urto.

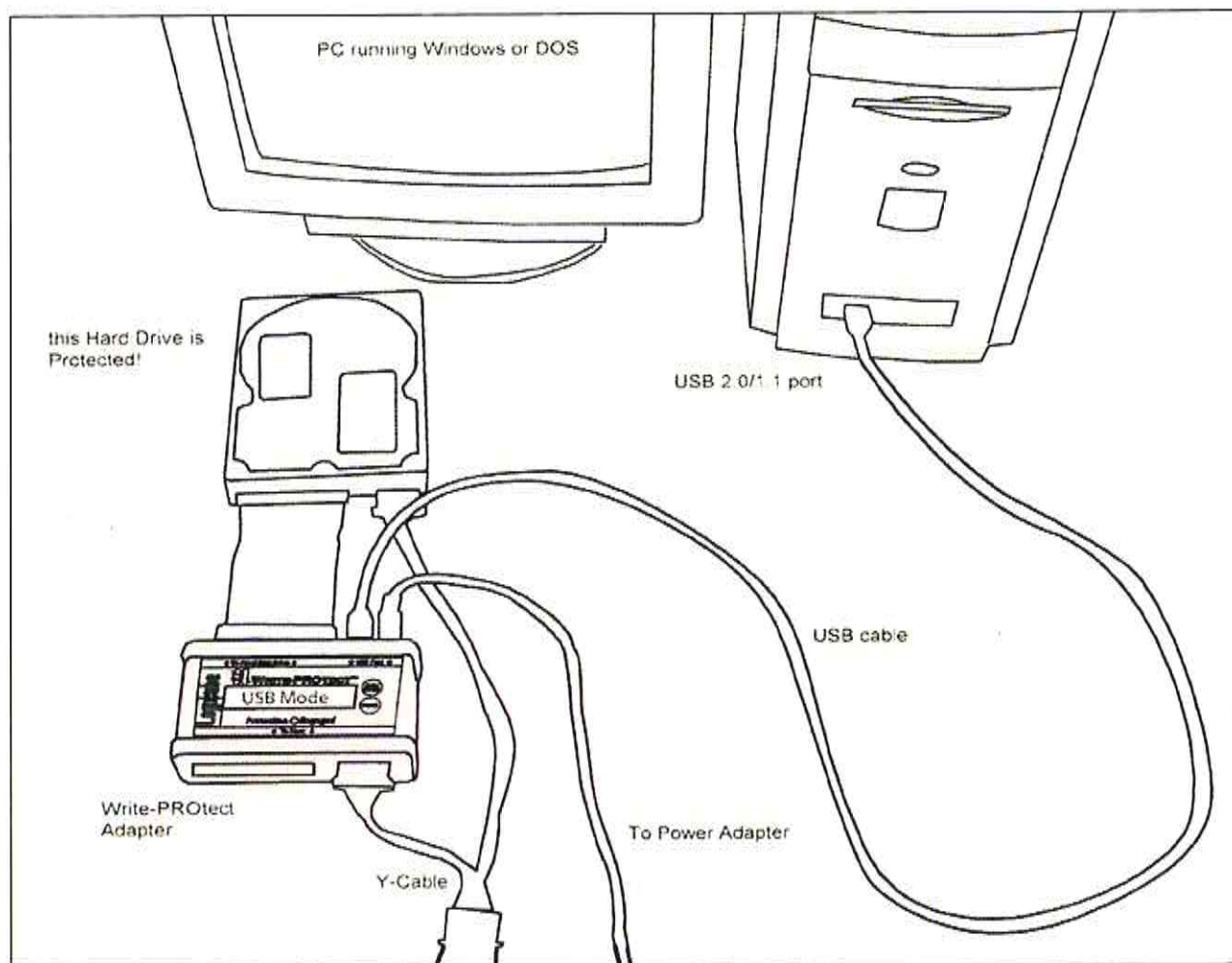
L'apparecchio è provvisto dei seguenti elementi:

- dispositivo Write-Protect™;
- alimentatore;
- cavo di connessione specifica per hard-disk;
- adattatore per hard- disk da 3 pollici e mezzo a 2 pollici e mezzo.

§ 5 – ATTIVITA' SVOLTA E RISULTATI CONSEGUITI

Come prima fase dell'esame dello strumento, è stata eseguita la normale procedura di collegamento alla rete elettrica, verificando preventivamente che le componenti dell'apparecchio (alimentatore - cavi di collegamento) fossero integre e prive di modificazioni e/o deterioramenti. A questo punto, si è collegato al dispositivo un adattatore necessario per l'interfacciamento con hard disk con attacco da 2 pollici e mezzo.

Il dispositivo è stato collegato per la lettura degli hard disk ad un personal computer, come mostrato nella seguente rappresentazione grafica.



Al riguardo, si precisa che per l'espletamento dell'incarico è stato utilizzato:

- ✓ computer e strumentazione hardware e software appartenente allo scrivente e al Servizio Polizia Postale e delle Comunicazioni.
- ✓ Un hard disk di capacità e tra cui uno da 120 gb acquistato appositamente, su autorizzazione di codesta A.G., e altri due hard disk di analoga marca e capacità di quelle sottoposte a sequestro.

Tenuto conto delle considerazioni espresse dal Prof. Bernaschi (consulente del GIP) circa le possibili cause di danneggiamento degli hard-disk, si è proceduto a collegare gli hard disk, dapprima nelle modalità corrette. In questo modo si è accertato il normale funzionamento del dispositivo. A questo punto, sono state effettuate numerose prove, finalizzate ad analizzare il comportamento del dispositivo di blocco anche in presenza di errori di collegamento da parte dell'operatore (disallineamenti dei pin rispetto al connettore ed inversione di polarità).

Per una più agevole disamina da parte di codesta A.G., si mostrano nelle figure 2 - 3 - 4 e 5 i collegamenti errati sottoposti a verifica.

In particolare, nelle figure 2 - 4 - 5, si raffigurano i disallineamenti sperimentati. Da tali prove emerge che il dispositivo, in queste situazioni, sebbene non consenta l'accesso al disco, impedisce che questo venga danneggiato.

Inoltre, nella figura 3, è stata evidenziata la particolarità dell'apparecchio, in virtù della quale, se l'operatore inverte per errore la polarità dell'alimentazione, lo strumento attiva un sistema di protezione che interrompe immediatamente l'erogazione dell'alimentazione all'hard disk, impedendo in questo modo un possibile danneggiamento dello stesso.

CONCLUSIONI

Sulla base delle risultanze sperimentali ottenute, si conclude che, il disallineamento dei pin del disco con quelli del connettore di collegamento dispositivo Write-Protect, in virtù delle protezioni elettriche implementate dal dispositivo Logicube Desktop Write Protect, non determina uno shock elettrico sull'hard disk.

Infine, anche alla luce delle rilevazioni con il tester sopra descritte, si esclude che il predetto dispositivo abbia erogato un'alimentazione con caratteristiche di tensione diverse da quelle previste.

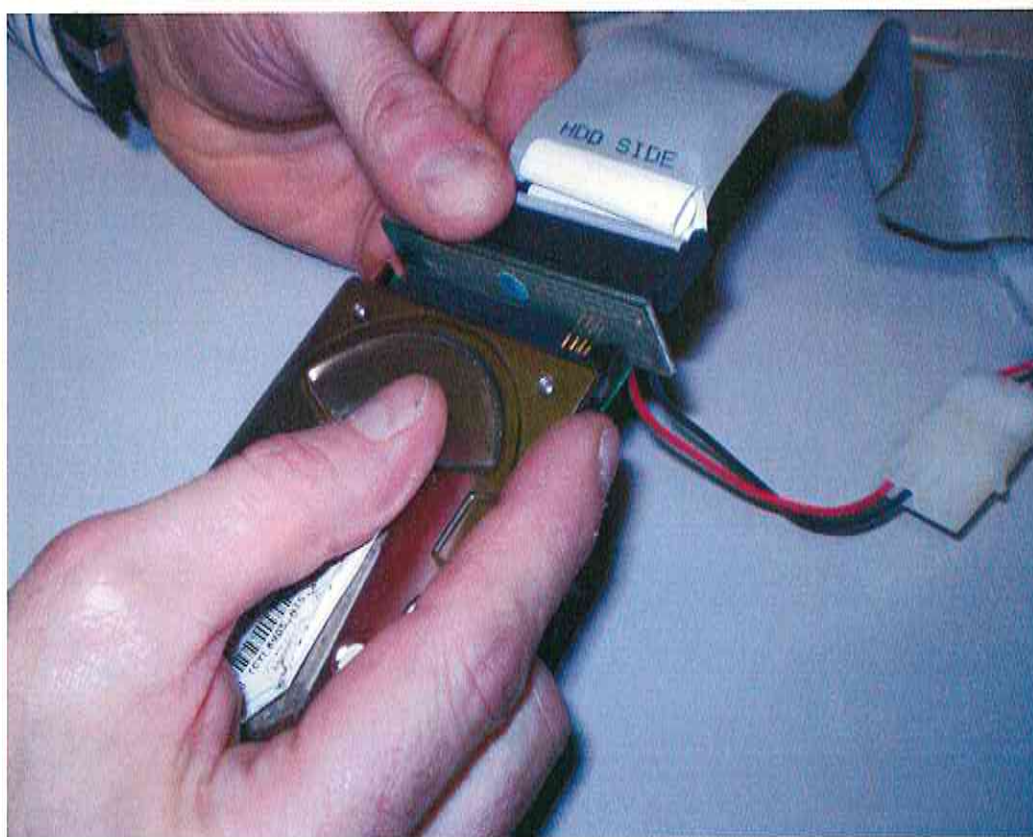


Fig.2

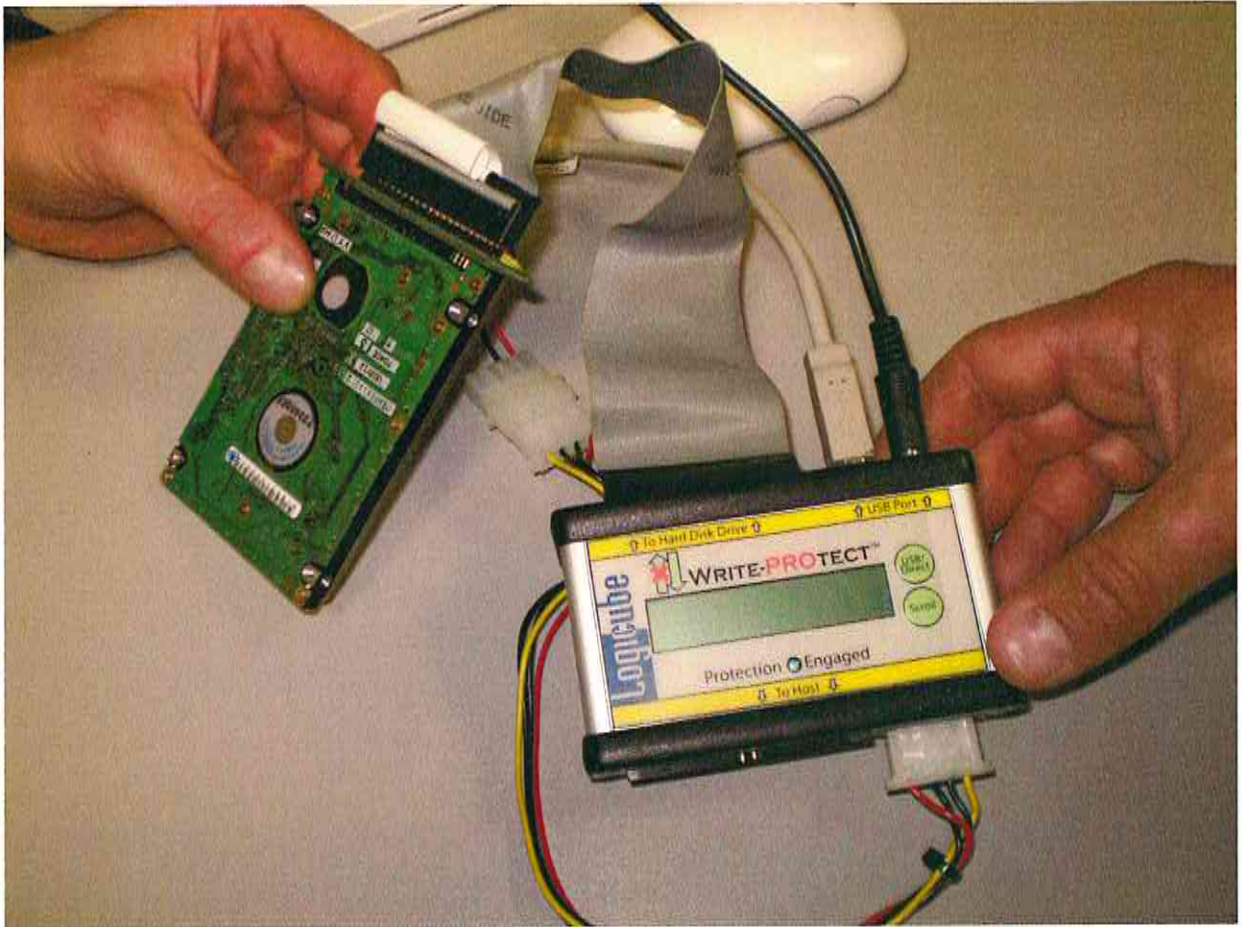


FIG 3

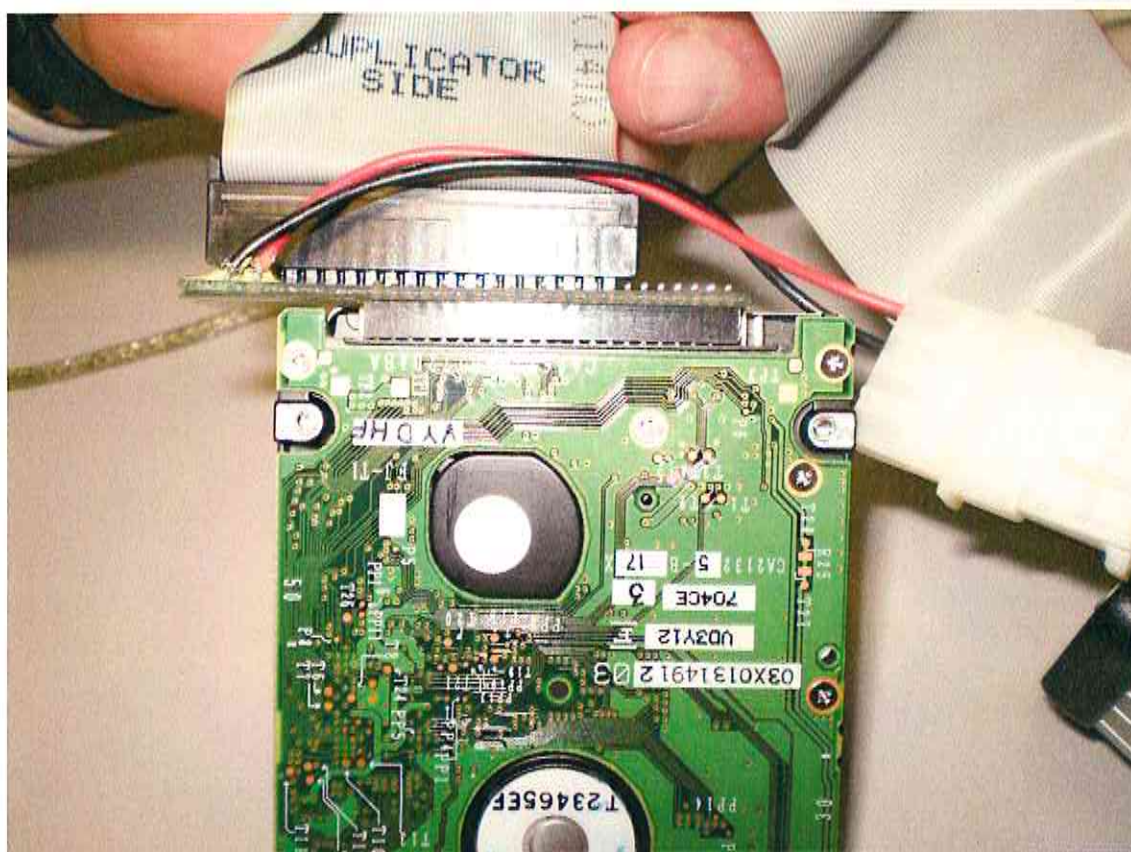


FIG.4

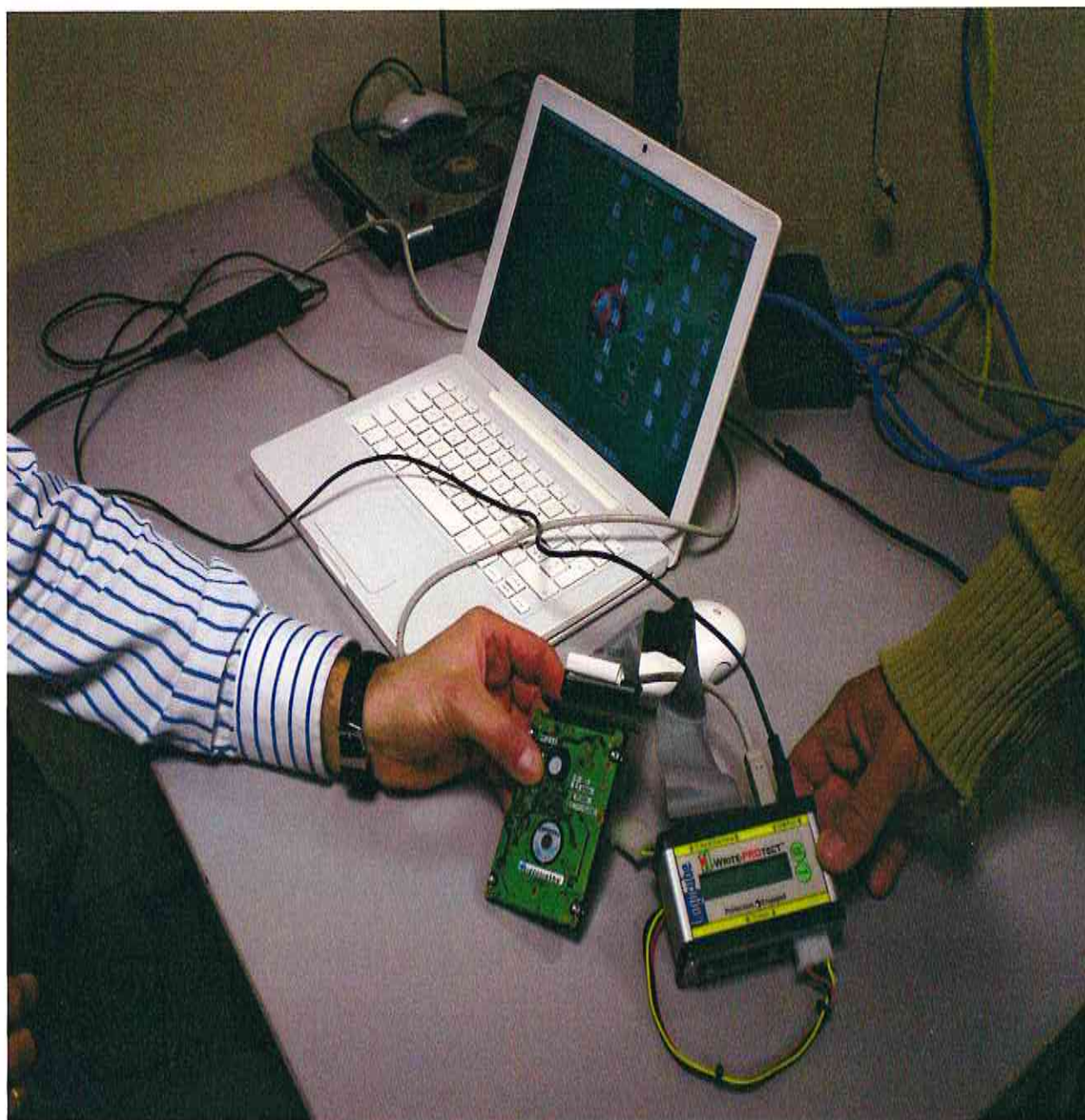


FIG.5

Roma, 23 aprile 2008

Il Consulente
Ispettore C. di P.S.
Mario GATTONE