

Shadow 2 von VOOM Technologies im Test

Eine vielschichtiges Problemfeld (nicht nur) der Computer Forensik ist die Vermittlung teilweise komplexer Ermittlungsergebnisse einem mehr oder weniger sachverständigem Publikum. Es sind manchmal Magierfähigkeiten notwendig, einem Laien technische Details über Cookies, Slack-Space, Registry, DLL, MAC-Timestamps oder die Funktionsweise von Software zu erklären. Die amerikanische Firma VOOM Technologies hat genau für diesen Zweck eine Hardware mit dem Namen **Shadow 2** auf den Markt gebracht.

Wir hatten das Teil bei uns im Labor zum Test und mein Kollege Sebastian Krause hat es für die [Zeitschrift iX](#) einem technischen Review unterzogen. Näheres dazu in Heft 10/2006. Zur Einstimmung hier ein paar Infos:

- Die Shadow2-Box wird zwischen Analyse-PC und dem verdächtigen Datenträger geschaltet (es fungiert auch als klassischer Writeblocker - wer 1.800\$ dafür ausgeben mag)
- Die verdächtige Platte kann normal gebootet werden, Lesezugriff ist transparent, Schreibzugriff **scheinbar** auch. Jetzt kommt aber der Clou: die Shadow2-Box führt die Schreibzugriffe nicht aus, sondern speichert sie auf einer eigenen internen Festplatte. Die verdächtige Festplatte wird nicht verändert, alle Schreibzugriffe finden nur in der Shadow2-Box statt.
- Skeptisch wie wir nun mal sind, haben wir auch mit einer HPA und mit DCO herumgespielt: Der Prüfsummenvergleich zeigt, dass der verdächtige Datenträger nicht verändert wurde.

Wozu nun das Ganze? Mit der Shadow2-Box kann man einen verdächtigen PC vor Gericht booten und das Original-Verzeichnis oder die Original-Anwendung zeigen und nicht nur nachstellen. Ist sozusagen eine Alternative zu Live View oder ProDiscover wo man ein VMware-Image eines Datenträgers erstellen kann, um sich das ganze dann unter VMWare-„Bedingungen“ anzuschauen. Man hat mit der Shadow2-Box das gleiche „Bild“ wie der User des verdächtigen PC. Ein anderes Einsatzszenario ist der Preview der Beweismittel im laufenden Betrieb, bevor man den Imager anwirft.

Leider konnten wir die Shadow2-Box nicht im Labor behalten, der deutsche Reseller wollte das Teil wieder zurück haben

CREDIT: www.computer-forensik.org; article: <http://computer-forensik.org/2006/09/29/hokus-pokus-mit-voom-shadow-2/>

Test of Shadow 2 by Voom Technologies

A multidimensional problem (not only) of computer forensics in part is to convey complex investigative results when your audience is unknown. Sometimes the skills of a magician are essential to explain to a lay person the technical details about cookies, slack space, registry, DLL, MAC timestamps or the functioning of software. The American company Voom Technologies has brought to market a hardware unit named **Shadow 2** for exactly this purpose.

We had a unit in our laboratory to test and my colleague Sebastian Krause performed a technical review for the [magazine iX](#). For details see Bulletin 10/2006. [http://www.heise.de/kiosk/archiv/ix/2006/10/72_kiosk] To familiarize oneself here is some info:

- The Shadow2 unit connects between the analysis PC and the suspect disk. (It also acts as a classical Write Blocker - who likes to spend \$1,800 for that purpose?)
- The suspect disk may be booted normally, read access is transparent, even **seemingly** write access. But now comes the trick: the Shadow2 unit does not execute the writes, rather it stores the writes on its own separate internal hard drive. The suspect hard drive is not changed, instead all write accesses can be found only in the Shadow2 unit.
- As we are highly skeptical, we also played around with an HPA and a DCO: the checksum showed that the suspect disk was not changed.

What's the big picture? With the Shadow2 unit you can boot a suspect PC in court and show the original directory, or the original application and not just re-enact the crime. It's a good alternative to Live View or ProDiscover where you create a VMware disk image and view the whole thing under VMware "conditions." The Shadow2 unit provides the same "image" as the user of the suspect PC. Another deployment scenario is to preview the evidence in the current case before capturing an image.

Unfortunately, we could not keep the Shadow2 unit in our laboratory, the German reseller wanted to have it back.