Uppgift

Ditt jobb är som bekant att utreda och analysera digitala kriminaltekniska bevis. Bevisningen är i detta fall en spegelavbild av en hårddisk.

Innan du börjar med uppgiften det är nyttigt att läsa polisanmälan m.m. för att få del bakgrundsinformation (precis som i alla andra undersökningar). Nu är bakgrundsinformationen i detta fall inte så omfattande utan all information är beskrivet i nedanstående scenario.

Scenario

De datasäkerhetsansvariga på ett företag har relativt starka misstankar om att en anställd dataanvändare sysslat med otillåtna aktiviteter på jobbet enligt följande lista:

- Sniffat datatrafik på företagets nätverk
- Installerat bakdörrar på sin egen PC
- Stulit och kopierat en CD-ROM med konfidentiellt innehåll
- Laddat ner copyright skyddad musik
- Använt ett pen-test tutorial dokument för att utföra en del av sina aktiviteter

När de datasäkerhetsansvariga beslagtog användarens PC var den avslagen och saknade den bootbara systemdisken. De tog dock en dd kopia på den hårddisk som satt kvar i datorn och sände den till dig för analys och utredning.

Du hittar spegelkopian här (7zip file): http://users.du.se/~hjo/cs/dt1019/lab/hdb1.7z
MD5 för spegelkopian är: 988654A1C7CC5AA5FB2FBBCA8A34504D

Inlämning

Försök att hitta så många bevis som möjligt av varje misstänkt aktivitet. Ge en beskrivning av de verktyg och den analys/process du använde för att finna dina bevis. Tänk på att bevisen kan vara maskerade på en rad olika sätt.

Förutsättningar

En förutsättning för denna hemuppgift är att enbart jobba med forensiska open source, gratis eller demo verktyg som FTK imager, The Sleuth Kit och Autopsy Browser, Pyflag och PTK (båda har The Sleuth Kit i botten), ProDiscover Basic Edition, ASR Data SMART. Sök på produkternas namn så hittar du senaste versionen.

En av de ledande tillverkarna av forensisk programvara i Europa, X-Ways Software har ett verktyg, Winhex som även finns i en forensic edition, då vid namn X-Ways Forensics - http://www.x-ways.net/. På [server]\tools\x-ways.net-winhex finns guider för hur man kommer igång med detta verktyg.

Andra systemverktyg som tex. montering av dd/raw till enhet med FTK Imager, Mount Image Pro/Paraben P2 eXplorer eller specifika Perl/Python script, antivirusprgram etc. osv. kan vara aktuella att använda.

Högskolan Dalarna
Röda vägen 3
781 88 BORLÄNGE

Telefon: 023-77 80 00
Telefax: 023-77 80 50
URL: http://www.du.se/

Kolla tex. på YouTube efter beskrivande videor i hur man använder dessa verktyg, det finns guider tex. för avancerad användning av WinHex.

VMware

En bra VMware image som SANS (http://www.sans.org/) använder under sina forensiska kurser har lagts upp på [server]\vmware\SIFT Workstation 2.12. Fullständiga namnet är SANS Investigative Forensic Toolkit (SIFT) Workstation och innehåller många forensiska verktyg, bl.a. PTK (http://ptk.dflabs.com/). Se readme.txt på [server] eller: http://computer-forensics.sans.org/community/downloads för login och användning etc. och bloggen nedan.

SIFT Workstation kanske är det bästa alternativet för din undersökning!

Bli gärna medlem hos SANS de har mycket läsvärt och användbart inom säkerhet och forensics speciellt på deras forensiska blogg: http://computer-forensics.sans.org/blog/

Slutord

Se till att gå igenom manualerna för programvarorna ordentligt så du förstår hur du ska använda dem effektivt.

Lycka till!

Högskolan Dalarna
Röda vägen 3
781 88 BORLÄNGE
Telefon: 023-77 80 00
Telefax: 023-77 80 50
URL: http://www.du.se/