Laboration 3

Du ska nu få planera och genomföra en komplett systemanalys, från live-respons till off-lineanalys. Först gör vi minnesdump och liveutvinning med hjälp av ett script. Därefter stänger vi ner systemet och genomför hårddiskutvinning. Slutligen så tar vi hjälp av programmet Autopsy och kopplar upp er mot avbildningen och analyserar filstrukturen och övrig data hos denna. Detta innebär bland annat att ni ska skapa en tidslinje för befintliga och borttagna filer, genomföra sökning efter nyckelord, sökningar med enkla reguljära uttryck samt jobba med hashvärden.

Konfiguration
Kopiera upp foldern Lab 3 från C:\VMW_template till C:\VMW. Starta maskinen som heter ”Windows”. När du får frågan om du kopierat eller flyttat maskinen anger du att du FLYTTAT den eller att du vill BEHÅLLA den oförändrad (move/keep). Du visas nu en meny där du kan välja mellan Windows och Ubuntu. Välj Windows. Maskinen startar upp, logga in med lösenordet forensics. Det är i detta läge som du påträffar datorn. Till datorn finns även denna gång en USB-disk med verktyg och utrymme för avbilder ansluten. Denna gång har du även tillgång till ett automatisk script för den initiala utvinningen.

Initial utvinning
Genomför en minnesdump. Titta igenom scriptet och repetera vad som kommer att ske när det körs. Glöm inte att analysera tidsavvikelsen manuellt. Gör en rimlighetsbedömning av loggarna från scriptet.

Stopp av systemet
Nu har vi genomfört vår initiala respons och ska gå vidare med datautvinning från hårddisken. När vi granskat det körande systemet så har vi kommit fram till att det är Windows XP samt att det inte handlar om någon server-variant. I detta läge förespråkar tumregeln att vi helt enkelt fattar tag i strömsladden på baksidan av datorn och drar ur.

Nu ska vi slarva lite och göra några fel. Börja med att kopiera en valfri fil till skrivbordet. Radera filen genom att trycka och hålla nere shift och tryck sedan på delete-knappen. Du har nu tagit bort en fil utan att lägga den i papperskorgen (en riktig delete). Trots att vi vet att vi borde dra ur strömkabeln väljer vi att istället stänga av maskinen från start-menyn.

Du har just brutit mot din egen policy. Vad måste du nu göra?

Uppstart av BackTrack
Vi ska nu stoppa i en DVD med BackTrack i datorn och starta upp systemet igen. Detta gör vi helt enkelt genom att starta maskinen som heter ”BackTrack” som ligger även den i foldern Lab 3. Nu visas en meny där du kan välja mellan Windows och Ubuntu. Välj Ubuntu. Systemet startar upp och frågar efter ett slag efter användarnamn och lösenord. Användarnamn är root och lösen är toor. Starta upp den grafiska klienten med startx. Kontrollera att din USB-disk finns monterad

Hårddiskutvinning
Genomför en hårddiskavbildning av hela disken med hjälp av air. Inställningarna ska vara följande:

- `src = /dev/sda`
- `dst = /mnt/toolbox/Images/windows.dd`
- `komprimering = none`
- `hash = md5`
- `verify = no`
- `use DCFLDD`

Spara sessionsdatat från statusfönstret efter utvinningen.

Hashset
Med hjälp av set av hashsummor så kan vi dela in filer i ”säkra” och ”intressanta” för att underlätta vårt fortsatta analysarbete. På er USB-disk finns redan ett färdigt hashset för ”säkra” filer, och ni ska nu skapa ett set för några ”intressanta” filer.
Ett hashset skapas genom att man skapar en lista med hashsummor för de filer man vill ha i sitt set och därefter kör man listan genom ett program som sorterar summorna för att underlätta och snabba upp sökningar (en så kallad indexering).
I foldern ”illegal_images” hittar du ett antal olagliga bilder som du nu ska använda för att skapa ett hashset.

1. Skapa hashsummor (ersätt /path med sökvägen till foldern med bilderna)
   `md5sum /path > illegal.db`
2. Genomför indexering.
   `hfind –i md5sum illegal.db`

Initiering av analys
Starta autopsy och skapa ett nytt case med följande inställningar:

- Case Name: HH-2010-MM-DD-002
- Description: Misstänkt informationsstöld.
- Investigator Names: Ditt Namn

Lägg till en host som representerar datorn ni gjort inhämtning från.

- Host Name: Comp-01
- Description: Eva Strands kontorsdator
- Time zone: Europe/Stockholm
- Timeskew Adjustment: ange tidsförskjutningen (i sekunder) du mätte upp under live-responsen. Ex. gick datorns klocka en minut före skriver du -60.
- Path of Alert Hash Database: ange sökvägen till ditt eget hashset (illegal.db)
- Path of Ignore Hash Database: du hittar denna fil i USB-diskens folder ”hashsets”.

Lägg till din hårddiskavbild till hosten.

- Location: sökvägen till din avbild.
- Type: Disk
- Import Method: Symlink

Koppla avbilden mot en checksumma samt ett filsystem.

- Data Integrity: Add + Verify hash. I rutan kopierar du in md5-värdet från air-loggen.
- Mount Point: C:
- File System Type: NTFS

Analys

När du använder autopsy tar vissa operationer lång tid. Håll ett öga på den lilla ”snurran” i övre högra hörnet. Snurrar den så arbetar autopsy.

Vi ska först av allt skapa en tidslinje av alla filer i systemet.

- Välj C:\ från Host Manager.
- Gå in under File Activity Time Lines
- Create Data File
    1. Markera C:\
    2. Tryck OK.
- Create Timeline
    1. Titta igenom de olika alternativen.
    2. Tryck OK
- View Timeline
    1. Prova att navigera lite i tidslinjen.
    2. Datat finns lagrat i en fil och det är enklare att använda en texteditor eller ett kalkylark för att titta på tidslinjen.
- Close

Vi ska nu göra en djupare analys av disken.

- **Analyze**, C:\, klicka därefter på **File Analysis**
    1. Prova på att navigera runt i filvyn uppe till höger.
- **Directory Seek**, vi kan hoppa direkt till en folder i systemet. Prova att hoppa till foldern windows/system genom att mata in sökvägen i rutan för Directory Seek (panelen till vänster) och klicka på View.
- **File Name Search**, vi kan söka efter filnamn och foldrar. Prova att söka efter cookies (sökrutan nedanför Directory Seek). Resultatet blir alla cookie-foldrar på disken.
- **File Views** i datafältet nere till höger. Vi kan här styra hur en fil ska visas. Om det är svårt att se allt så kan man ändra storleken på de olika ramarna.
    1. Sök efter comsetup.log. Klicka på filen. Nu visas filen som ascii-text. Detta är lämpligt för textfile och log-filer som denna fil.
    2. Gör en filsökning efter clock.avi. Klicka på filen. Nu visas filen som ascii-text. Klicka på Hex display. Detta är en bättre vy för binära filer.
    3. Gör en filsökning efter notepad.exe. Klicka på filen. Nu visas filen som ascii-text. Klicka på Hex display. Prova nu att klicka på Strings display. Detta plockar ut skrivbara tecken ur den binära filen och visar dessa. Detta kan användas för att tex. se olika inbäddade textmeddelanden i filer.
    4. Gör en filsökning efter RECYCLE (Windows Recycle Bin). Klicka dig nedåt i filstrukturen tills du inte kommer längre. Här finns en fil Dc1.jpg. Klicka på filen. Du ser nu en bild på några barn i förskoleverksamhet. Detta kan vara ett viktigt bevis och vi lägger till en notering. Klicka på Add Note och fyll i ”Bild på barn som leker. Utred dess sammanhang.”. Klicka Ok.

- **All Deleted Files**, näst längst ner i panelen till vänster. Detta verktyg gör det möjligt att visa alla raderade filer på disken. Klicka på filen du av misstag lade på Skrivbordet. Vi vill nu återställa filen. Gör detta genom att klicka Export. Du får nu välja en sökväg för vart du vill spara filen. Välj en lämplig folder i /mnt/toolbox. Vad bör du dessutom göra?
- **Expand Directories**, längst ner i panelen till vänster. Detta verktyg visar hela folderstrukturen på disken.
- **Keyword search**, nyckelordssökning är en central del i analysen av ett avbildat system. För att snabba upp sökningarna så gör vi först en strängutvinning genom att klicka på Extract Strings. Du kommer till en ganska lång sida med inställningar. Lämna inställningarna orörda och klicka på Extract Strings längst ner på sidan. Efter några minuter är utvinningen klar och du kan klicka på Keyword Search.
    1. Som ett exempel kan vi även göra en sökning efter e-postadresser. För detta kan ni använda uttrycket [A-Z0-9]+@[A-Z0-9]+\.[A-Z]{2,4} vilket i stora drag innebär att vi kommer att leta efter strängar med minst ett tecken följt av ett @, sedan minst ett tecken följt av en punkt, därefter 2 till fyra bokstäver. Tex. a@b.se eller nisse-hult@alsccch.info . Prova detta. Glöm inte att klicka i rutan för GREP-search. Det borde ge ca 1000 träffar.
    2. Vet vi tex. att användaren troligtvis kallar sig eva kan vi ändra på sökuttrycket och fråga efter e-postadresser som matchar eva[A-Z0-9]+@[A-Z0-9]+\.[A-Z]{2,4}.
    3. I just detta exemplet så har Eva Strand utövat utpressning mot en person och hotat dennes barn (bilden i papperskorgen). Under kursen Avancerade Forensiska Verktyg I kommer vi att granska detta närmare.
- **File Type**, med detta verktyg kan vi undersöka om man försökt dölja en fil genom att byta filändelse. Vi får även en automatisk slagning mot våra hash-databaseer. Anmärkning: Autopsy har stöd för detta men det fungerar inte så bra som man skulle önska.
    1. Starta sökningen genom att klicka på Ok.
    2. När sökningen är klar så kan du se statistik om hur filerna på disken katalogiserats. Intressantast just nu är kategorin Hash Databases. Du borde fått ca. 8 träffar i alert databasen.
    3. Klicka på View Sorted Files och kopiera/klistra in länken du får i en ny tab (ctrl-t).
    4. Klicka på länken Hash Database Alerts. Nu ser du de filer som identifierats på disken och som finns i databasen. Ett antal filer fanns i Temporary Internet Files. Vad innebär det? Ett antal filer fanns i Administrator/My Documents/My Pictures. Vad innebär det?
    5. Sök upp någon av de filer som inte har filändelsen jpg och undersök innehållet i dem. Skriv därefter en notering om filen, tex. ”Fil som är olaglig att inneha.”.
- **Data Unit**, detta verktyg gör det möjligt att navigera direkt bland kluster på disken.
- **Close**, låter oss nu gå tillbaka till Host Manager.
- **Image Integrity**, detta verktyg låter oss kolla att avbilden inte skadats genom att beräkna checksummorna på nytt. Bör göras ett antal tillfällen under arbetets gång.
- **View Notes**, detta verktyg gör det möjligt att se en sammanställning över de filer vi skapat noteringar för.
- **Event Sequencer**, gör det möjligt att lägga in händelser som inte syns i vårt system. Tex. tidpunkten då en viss attack påbörjades eller tidpunkten då ett mail togs emot.

Avslutning
Stäng ner den virtuella maskinen och radera dina filer.

För mer information, se även tex. http://tinyurl.com/2updwhp

(http://blogs.sans.org/computer-forensics/2009/05/11/a-step-by-step-introduction-to-using-the-autopsy-forensic-browser/)

Demonstration: EnCase