Laboration 2

Det huvudsakliga syftet med laboration 2 är att lära sig att göra en grundläggande dataanalys av en hårddiskavbildning. Med hjälp av programmet Autopsy så ska ni koppla upp er mot en avbildning av en okänd hårddisk och analysera filstrukturen hos denna. Detta innebär bland annat att ni ska skapa en tidslinje för befintliga och borttagna filer, genomföra sökning efter nyckelord, enkla reguljära uttryck samt hashvärden. Förutsättningen kommer att vara samma utgångsläge som för laboration 1, dvs. initial respons och forensisk kopiering måste göras innan avbildningen kan kopplas upp för analys.

1. Kopiera den virtuella maskinen från USB-stickan till D:. Skulle det vara för lite tomt utrymme finns ett rensningsscript i foldern D:\wmw
2. Starta den virtuella maskinen. Den startar automatiskt från hårddisken.
3. Logga in som administratör. Lösenordet är ide. Det är i detta läge du träffar på systemet.
4. Titta igenom scriptet i verktygslådan på E:\ och repetera vad som kommer att ske när det körs. Glöm inte att analysera tidsavvikelsen.
5. Genomför initial respons med hjälp av scriptet i verktygslådan.
6. Starta om systemet. Tryck escape innan Windows börjar ladda. Du får upp en boot-meny. Välj att boota från CD. Detta startar Helix. Välj att starta Helix i läge ”gui”.
7. Skapa en folder /media/b. Montera /dev/hdb1 till foldern /media/b.
8. Gör forensiska avbildningar av hda (stor) och hdd (liten) till /media/b, använd tex. Adepto. Se till att du sparar hashsummorna – du hittar dessa under fliken ”Log”.
9. Starta Autopsy.
10. Välj ”New case”. Mata in lämpliga uppgifter, tex. ”Lab 2”, ”Test av dataanalys”, ”Namn”. Klicka ”New case”.
11. Välj ditt namn i dropplisten. Klicka ”Add host”.
12. Fyll i lämplig information. Tidsinformationen hämtar du från din egen dokumentation. Som ignore-databas fyller du i /media/b/t.db och alert-databas lämnar vi tom. Detta är en databas som jag gjort i ordning just för denna labb men som kan bytas mot andra databaser som passar ert ändamål. Ignore = filer som är kända och ”vänliga” (systemfiler, programvaror…), alert = filer som är kända och ”farliga” (trojaner, klassad information…). Klicka ”Add host”
13. Nu ska vi lägga till avbildningarna. Klicka ”Add image” och välj ”Add image file”. Lägg till de båda avbildningarna. Se till att du väljer rätt typ av avbildning – eftersom du gjort avbildningar av hela diskar så klickar vi i ”Disk” som typ. Eftersom vi inte har några särskilda krav på hur avbildningen ska hanteras så låter vi import method vara ”Symlink”, vilket innebär att avbildningen ligger kvar och vi innan vi går vidare med ”Next”.
14. Nu får vi möjlighet att ange hur vi ska hantera integriteten hos avbildningarna. Eftersom vi har hasharna tillgängliga så markerar vi ”Add hash”, kopierar in rätt hash i rutan och klickar i att vi vill göra en kontroll att summan stämmer. Filsystemdetaljerna autodetekteras, men kontrollera för säkerhets skull att den stora disken får typen NTFS och den lilla FAT16. Ange monteringspunkten för den stora disken till C: och den lilla till D:.
15. Klicka ”Add image” och upprepa för den andra avbilden. Välj sedan ”Ok” för att gå vidare. Nu får vi möjlighet att markera en av avbilderna och göra vidare analys. Vi börjar med att markera C: och klicka ”Analyze”.

16. Vi ska till att börja med jobba med dataanalys av filsystemet och klickar därför ”File Analysis”. Du får upp en filbläddrare med en meny till vänster och ett datafält nedtill. Prova på att navigera runt lite i filbläddraren för att skaffa lite känsla för hur den fungerar. Klicka på ”Help” och välj ”File Analysis” för detaljer.
17. Klicka på filen C:\ntdetect.com. Filens innehåll visas i datafältet och ett antal visningslägen anges. Prova alla tre (ASCII, Hex och ASCII String). Vad innebär de olika visningslägena? Vad kan de vara bra för?
18. Prova att göra en rapport i visningsläge ”ASCII String”. Undersök hur rapporten är konstruerad och vilken information vi kan hitta.
19. Med hjälp av ”Export” kan vi extrahera en fil från avbilden för vidare bearbetning. Gör detta. När kan det vara användbart?
20. Nu ska vi undersöka borttagna filer. Som du kan se i sidomenyn så finns det en funktion för att samla alla borttagna filer i en enskild vy. Klicka på ”All deleted files” och låt listan fyllas i.
21. Leta reda på filen ”…/Cookies/index.dat” i början av listan. Detta är en loggfil från ett webläsarprogram och kan givetvis innehålla mycket intressant information om vart användaren har surfat och i vissa fall till och med lösenord. Filen är raderad och skulle kunna vara det av lite olika skäl, till exempel så kan användaren vara medveten om att det lagras känslig information i filen och därför tagit bort den, men det förekommer även att webläsaren själv ordnar om i sina filer. Ta en närmare titt på filen. Vilket visningsläge är lämpligt och för vad? Extrahera filen.
22. Vi vill nu göra en notering om att vi funnit att denna datafil hade raderats. Gör detta genom att klicka ”Add Note”. Fyll i information om filen i rutan och klicka i den viktigaste tidsstämpeln av m, a och c. Motivera ditt val.
23. Välj ”View notes” och sedan stänger du fliken och återgår till filanalysläget för C:\.
24. Gå till C:\Windows\System och välj valfri fil. Vi antar att vi misstänker att just den filen kan vara en trojan eller innehålla dold information. Klicka på länken i filens metadata-kolumn (ute i högerkanten). Du får nu upp en vy över filens metadata. Här har du möjlighet att kontrollera om filen finns med i Ignore- eller Alert-databaserna. Som jämförelse kan du ta och upprepa detta för filen index.dat som vi arbetade med under punkt 21. Fanns filerna med i databaserna? Gör en anteckning med ”Add Note” huruvida du kunde avfärda din misstanke.
25. Stäng nu filbläddraren med knappen ”Close” och byt analysobjekt till D:\.
26. Vi ska nu göra mer generella sökningar i datat och går därför till ”Keyword search”. Detta är ett enkelt sökinterface som i enklaste form kan söka efter text men i sitt avancerade läge kan göra mycket komplexa mönstermatchningar. För att snabba upp sökningarna så väljer vi först att extrahera alla strängar med hjälp av ”Extract Strings”. Detta kan ta några minuter men gör att våra enskilda sökningar blir avsevärt snabbare.
27. Börja med att söka efter ”kill”, klicka i ”Case insensitive” så vi får med alla varianter av ”kill” (Kill, KILL…). Du får upp en lista till vänster med smakprov på träffarna i de olika klustren på disken. Som du ser är det många träffar på ord där kill ingår, tex. skillnader.
28. Detta var ju inte riktigt vad vi ville åstadkomma så vi gör om sökningen men med ett reguljärt uttryck. Klicka nu även i ”grep” och fyll i sökordet \bkill\b. \b är ett kontrolltecken som betyder att ordet kill måste omges av avgränsare i någon form och då inte får vara del av ett ord. Vi reducerar effektivt antalet träffar från 12 till 2.
29. På disken ligger ett antal chattloggar med tidsstämplar. Anta att vi vet ungefär när i tiden då intressant information framförts och vi vill leta efter detta. Tidsstämpeln i chattloggen ser ut som följer [HH:MM] där HH är timma och MM minuter. Anta att

vi vill sotera ut tidsstämplar mellan 11:20 och 11:29. Sökuttrycket för detta blir 11:2. (observera punkten). Prova detta. Kontrollera att träffarna verkar att stämma. Vilka problem kan du tänka dig att en sådan sökning kan resultera i?

30. 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@als.cc-ch.info . Prova detta. Det borde ge ca 500 träffar.
31. Vet vi tex. att användaren troligtvis kallar sig michiel kan vi ändra på sökuttrycket och fråga efter e-postadresser som matchar michiel@[A-Z0-9.-]+\.[A-Z]{2,4} .
32. Genom att välja en av träffarna och klicka på länken ”Find Meta Data Adress” kan vi få fram i vilken fil vi hittade detta data. Gör noteringar om att en misstänkt e-postadress påträffats för de två träffarna vi fick för michiel genom att klicka på ”Add note”. Avsluta sedan analysdelen genom att klicka på ”Close”.
33. Vet vi när något inträffat eller vi bara vill se data ur ett tidsperspektiv så kan vi välja att extrahera en ”File Activity Timelines”. Klicka på knappen med samma namn och sedan ”Create Data File”. Välj att extrahera från D:\ och gå vidare med ”OK”. Efter ett slag kommer information om att operationen lyckades och du kan gå vidare med ”OK”. Vi får nu möjligheten att skära ut ett litet snitt i tiden för att skapa vår tidslinje. Välj dagens datum som slutdatum och tryck sedan ”OK”. Information om operationen visas och du kan gå vidare med ”OK”. Här får du nu en vy över filerna i tidsordning. Förutom att ger en bra översikt så kan man dessutom lägga in kända tidpunkter som noteringar och på så vis enklare få grepp om när saker skett.
34. Vi vill nu göra en undersökning av filerna på disken baserat på deras faktiska innehåll. Autopsy har stöd för detta men det fungerar inte så bra ännu. Därför gör vi denna sista del i ett program som heter Retriever. Skapa en katalog som heter /media/d. Montera /dev/hdd1 till /media/d. Starta Retriever. Ta bort elementet i rutan ”Search path” med ”Remove”. Lägg till /media/d till sökvägen med ”Add”.
35. Nu ska vi söka efter bildfiler så därför klickar vi på fliken ”Graphics” och sedan ”Search”. Detta leder till att hårddisken letas igenom efter filer som datamässigt matchar hur en bildfil bör se ut. Dvs. om någon försökt gömma en bildfil genom att byta namn på den kommer vi att hitta den här.
36. Det visar sig att man försökt att dölja en fil på just detta sätt. Bilderna går att granska via ”View”. Filen som man bytt namn på kan granskas genom att man högerklickar på den i vyn ”View” och väljer ”Open with…” och anger kommandot ”display”, alternativt att man döper om filen.
37. Stäng ner den virtuella maskinen och ta bort filerna från hårddisken.