Computer Forensics, Del 1

Computer Forensics er kunsten at finde skjult data, at genskabe tabt data samt at undersøge filers fuktionalitet og formal. Denne artikel er den første i en serie. Artiklen henvender sig til den seriøse og øvede IT bruger/Administrator

Skrevet den **03. Feb 2009** af **bufferzone** I kategorien **Sikkerhed / Generelt** | ★★★☆☆

Computer Forensics

Computer forensics er et nyt emne under IT sikkerhed, jeg har kastet mig over og jeg arbejder frem mod en GCFA certificering (Se www.giac.org). Det er min hensigt under min behandling af emnet at skrive en lille serie af artikler, der forklare principperne, beskriver brugen af værktøjer og procedure på en måde så andre relativt hurtigt kan sætte sig ind i dette spændende emne.

Computer Forensics, Del 1: http://www.eksperten.dk/artikler/616
Computer Forensics, Del 2: http://www.eksperten.dk/artikler/685

Hvad er computer forensics så

Computer forensic er de undersøgelses- og analyse teknikker man anvender for at afdække og sikre potentielle beviser i computer relateret kriminalitet, hvad enten vi taler om kriminalitet i lovens forstand med retslige beviser eller vi taler om kriminalitet i forhold til forretnings-, ansættelses og kontraktsmæssige forhold eller vi taler om decideret industri spionage.
Disse beviser, retslige eller andet, findes med andre ord inden for en bred vifte af computerrelateret brug, f.eks. forretningshemmeligheder, tyveri af eller ødelæggelse af immateriel ejendom, svindel, afsløring eller tyveri af fortrolig data og meget andet.

Håndtering af beviserne (filer, data) er meget vigtigt, især hvis den analyse og undersøgelse man laver skal, bruges i retslig sammenhæng. Følgende er vigtigt

1. Det er selvfølgeligt afgørende at man ikke skader, ødelægger eller ændre beviserne med de procedure og teknikker man anvender. Alene sandsynliggørelsens af, at de procedurer man har anvendt ikke tilstrækkeligt sikre dette, er nok til, at det man finder, ikke kan bruges i retten. Ofte anvendes checksumme til at vise at filen ikke er blevet ændret f.eks. efter at være blevet flyttet fra forskellige medier.

2. Det er vigtigt at systemet der undersøges, ikke "forurenes" med filer og andet f.eks. virus. De anvendte procedure SKAL sikre dette, ellers er beviserne uanvendelige i retslig sammenhæng. Igen anvendes checksumme og forskellige lister og oversigter af indhold, filstørrelser og andet.

3. Det er vigtigt at alle fund og beviser beskyttes mod senere mekanisk eller elektronisk ødelæggelse. Beviser skal kunne genskabes fra det sikrede oprindelige system og det skal kunne bevises at der er tale om uændrede data, se ovenfor.

4. Etablering af chain of custody er afgørende hvis beviser skal bruges retsligt. Etablering af chain of custody betyder, at der er dokumentation for hvad der fysisk er sket med beviserne siden de blev modtaget og fremad. Hvor har beviserne befundet sig, hvem har haft dem i varetægt, hvem har haft ansvar for dem, hvordan er de blevet opbevaret osv. osv.

5. Alt skal dokumenteres. Hvad du gør, hvilke værktøjer du anvendes, hvordan de anvendes, hvilke filer der finders, hvor og hvordan de findes. Systemets fil struktur, osv. osv. osv. Ligegyldig hvor meget du dokumenterer, ville du efterfølgende ønske at du havde dokumenteret mere

6. Endelig er det selvfølgelig ofte vigtigt for virksomheden at den dels kan videreføre sine forretninger uhindret, samt at e.v.t. brud på sikkerhed, herunder primært konfidentialitet og integritet er sikret

Forensic specialister anvender en lang række af metoder, procedure og værktøjer for at finde skjult data, genskabe tabt data, bevist eller ubevist ødelagt data, frembringe krypteret data, password beskyttet data, data på swap-partitioner eller -filer, data i midlertidige filer, data på specielle områder af diske eller filer. Ligeså forekommer det også ofte at ukendte filer, f.eks. binære filer eller eksekverbare filer skal analyseres med henblik på at kunne afdække hvad disse filer gør og hvem der har haft fat i dem. Beskyttelse at disse filer følger de samme retningslinier som ovenstående

Hvor kan filer gemmes

Filer kan faktisk gemmes forbavsende mange steder på elektroniske medier af forskellig slags. Jeg har herunder brugt de engelske betegnelser således at du kan finde yderligere information ved at søge med f.eks. google.

File Slack
Slack space opstår når en fil ikke udfylder hele den/de allokerede clusters (hvilket de I praksis aldrig gør). Når en fil gemmes på et medie placeres den i et antal clusters og normalt fyldes den sidste cluster ikke helt ud. Hvis filer vokser i størrelse (du skriver f.eks. nogle sider mere på dit dokument) vil der blive fyldt i den sidste cluster, indtil denne er fuld, hvorefter endnu en cluster allokeres til filer. Den plads der er tilbage i den sidste cluster, kaldes File Slack, og her kan man dels finde data fra tidligere gemte og nu overskrevne filer og her kan også gemmes date bevidst på dette område at mediet.
File slack kan også indeholde rå data fra memory dumps der sker når filer lukkes ned.

Unused Space
Unused clusters er clusters der endnu ikke er blevet udfyldt med filer. Her kan der ligesom i File Slack gemme sig data der tidligere er blevet slettet samt data der bevidst er gemt her for at det ikke skal kunne findes let. Alle filer der gemmes på et medie indskrives i master boot record'en (MBR). Når du sletter en fir, sletter du i virkeligheden kun optegnelsen i MBR. Filen står således stadig på disker og kan genskabes med de rigtige værktøjer

Inter-Partition Space
En harddisk skal partitioneres for at den kan bruges og den kan deles op I en eller flere partitioner ligesom man kan undlade at partitionere dele af disken. Inter-Partition Space er de områder af mediet der ikke indeholder en partition. På disse områder kan der ligge spor og data fra tidligere partitioner ligesom der kan gemmes data her bevidst.

Swap file space
Windows sletter ikke data der placeres I swap filen. Data overskrives dynamisk efterhånden som ny data placeres i swap filen, men når systemet slukkes, fjernes/slettes swap data ikke. Dette betyder at swap filer kan være en god kilder til at finde dataspor og data der er slettet, eller ikke har været gemt på diske eller andre medier.

Storage Anomalies
Undersøgelse af filer for mistænkelige ting og anormaliteter kræver selvfølgelig erfaring. Man er nødt til atvide hvad der er normalt for at kunne se det ikke normale. Hvis man f.eks. tinder en .txt fil, der fylder 15 Mb, men kun indeholder 5 liniers tekst og ingen billeder, bør dette vække mistænksomhed. Man bør være opmærksom på alle forhold omkring filer for at kunne se de, ofte få og diskrete indikationer på, at der er noget galt.

Steganografi
Steganografi er kunsten at gemmer informationer i andre informationer. Den mest almindelige form for steganografi er vandmærker, der jo anvendes på pengesedler, frimærker og mange andre officielle dokumenter for at kunne verificere deres ægthed.
Når vi taler om steganografi i fil sammenhæng, er det mest almindeligt at den data der skal skjules, gemmes/skjules/indlejres i mediefiler, f.eks. digitale billeder, lydfiler eller filmklip. Den data der skal skjules, bliver gemt på "mindst betydende bit". I praksis betyder dette, at du f.eks. ikke umiddelbart kan se på billedet, at der er skjult data I det, men sammenligner du billedet med den skjulte data med originalen, vil du kunne se et kvalitets fald i det billedet med den skjulte data. Hvis du ikke har original filerne at sammenligne med, er du nødt til at undersøge alle mediafiler for at kontrollere om de skulle indeholde skjult data. Og da du ikke på forhånd kan vide hvilket værktøj der er anvendt til at skjule med, er denne opgave ikke noget man gør sådan uden videre.
Jeg overvejer om jeg skal give en teknisk forklaring på "Mindst betydende bit" i en senere artikel.

General Evidence Processing Guidelines (Provided by New Technologies, Inc.):

1) Sluk Computeren
Dette bør gøres hurtigst muligt for at sikre at e.v.t. destruktive processer der kører I baggrunden ikke får tid til at ødelægge mere end nødvendigt. Tag om nødvendig strømmen

2) Dokumenter Systemets Hardware Konfiguration
Sørg for at dokumentationen for hvordan systemet er sat sammen er så grundig at den kan genskabes fuldstændigt senere under sikrede forhold. Digital kameraer kan være en stor hjælp her.

3) Transport af Computer Systemet til sikre forhold.
Etablering af chain of custody starter når forensic holdet ankommer. Herfra skal bevisernes placering og tilstand kunne dokumenteres. De må ikke efterlades uden fuld kontrol eller opsyn af autoriseret personel.!

4) Lav Bit Stream Backups af alle medier. Hard Disks, Floppy Disks, Tape drives, USP keys og andet.
Da systemet ikke kan tændes uden at data måske ændres eller ødelægges er en Bit Stream Backup kopi nødvendig for at kunne analysere disse medierne. Originale medier og den første Original Bit Stream kopi gemmes under sikrede (og meget gerne geografisk separate) forhold og alle analyser gennemføres på et reference system etableret fra Bit Stream kopier.

5) Matematiske Check summer på alle data og medier.
For at kunne bevise at intet er ændret i forholdt til de originale beviser tages checksummer af alt. Der findes værktøjer til dette der kan gøre det på et acceptabelt sikkerhedsniveau

6) Dokumenter System Date og Time
Datoer og tid er meget vigtigt ud fra et retsligt synspunkt. Da handlinger og begivenheder skal kunne relateres til logfiler fra andre kilder, f.eks. ISP-, router-, firewall eller syslog server, er det væsentligt at disse indsamles, sikres med checksummer og at de er så nøjagtige som muligt.

7) List relevante Key Words

En viden eller mistanke om hvem personen vi har med at gøre og hvad emnerne drejer sig om, kan ofte give os en liste med relevante søgeord, der kan hjælpe i den senere efterforskning. Denne liste opstår ved at interviewe alle relevante personer.

8) Undersøg Windows Swap File

9) Undersøg File Slack

10) Undersøg Ikke allokeret Space (Slettede filer)

11) Gennemsøg Filer, File Slack og Ikke allokeret Space for Key Words
The list of relevant key words identified in the previous steps should be used to search all relevant computer hard disk drives and floppy diskettes.

12) Document File Names, Dates and Times
Dette er der værktøjer der kan gøre. Med erfaring kan listen af søgeord blive længere og dermed et meget brugbart værktøj.

13) Identificer Filer, Programmer og Storage Anomalies
Krypterede, komprimerede, eksekverbare grafiske og andre filer gemmer data i binær form. Disse filer kræver manuel undersøgelse med relevante værktøjer

14) Undersøg Programmer og Eksekverbare filers Funktionalitet
Vi taler her både om undersøgelse af funktionalitet, processer og kommunikation.

15) Dokumenter alt.
Alt skal dokumenteres, valideres og integritetssikres så det kan genskabes på en troværdig made. Dokumentation af bade procedure og hvad der findes. Checksum validering af data, filer og værktøj. Selv de værktøjer du anvender, skal valideres med Checksummer så det kan beviser at værktøjer, er der rigtige og ikke ændret.

16) Lav sikrede kopier af alt anvendt Software.
Samtidig med at der tages Checksum af alt det anvendte software gemmes kopier af dette og der etableres en chain of custody på same måde som med beviser. Disse software kopier kan ende med at blive beviser.

Det var så den første artikel i hvad der sandsynligvis bliver en serie. Denne artikle handler om at få emnet på plads, næste artikel vil tage fat på værktøjer og procedure og dermed blive meget mere håndgribelig.

Hvis du har kommentarer og/eller spørgsmål, er du velkommen til at kontakte mig på kim@bufferzone.dk lige som jeg selvfølgelig er at finde på Eksperten. Jeg modtager kommentarer og rettelser (f.eks. af stavefejl) med tak. Jeg beder om at du ikke stiller spørgsmål i kommentarerne til artiklen, der kan jeg jo ikke besvare dem.

Kommentar af cyberfinn d. 15. Feb 2005 | 1

En rigtig god artikel om emnet. Glæder mig til den næste i serien.

Kommentar af brixz d. 26. Oct 2005 | 2

Kommentar af j_jorgensen d. 16. Feb 2005 | 3

Artiklen er udemærket, den går dog ikke i detaljer med værktøjerne. Det er meget generelle beskrivelser af fremgangsmåderne.

Kommentar af lenk d. 09. May 2005 | 4

God appetitvækker, hvis hovedretten lever op til forvendtningerne blever det godt

Kommentar af dreamless d. 15. Feb 2005 | 5

God artikel, lidt stave/slåfejl.

Kommentar af frewald d. 04. Mar 2005 | 6

Spændende læsning, men jeg savner reele værktøjer.

Kommentar af aros d. 15. Feb 2005 | 7

Kanon artikel, har dog lidt svært ved at læse alt teksten på den sidste del af artiklen, det er som om noget af teksten forsvinder ud i marginen

Kommentar af over-load d. 22. Apr 2005 | 8

glæder mig til de næste artikler i serien :)
pas lige på med typoes ;D, og lidt mere om andet end det generelle ville også hjælpe

Kommentar af petkrug d. 15. Feb 2005 | 9

Som sædvanligt en rigtig god og godt forklarende artikel fra bufferzone. Man kan jo mærke at dette er et emne manden brænder for og som han faktisk har tilegnet sig en dyb og respektindgydende viden om. Keep up the good work....//PetKrug

Kommentar af optical d. 21. Feb 2005 | 10

synes ikke den holder sig til buffer_zone standart, men ellers udemærket

Kommentar af alister_crowley d. 16. Feb 2005 | 11