Angivelig lekkasje av politimateriale

"Terrorsaken"

Versjon 2.7. Denne versjonen er en omarbeidet versjon av den opprinnelige rapporten (Versjon 1.5) av 23.06.2012. Rapporten oppsummerer og erstatter alle tidligere utgaver av samme rapport.

Enkelte kapitler er nye som følge av at ny informasjon og dokumentasjon er fremkommet. Dette dreier seg særlig omkring forhold rundt tidslinjen.

Det er lagt inn et "Vedlegg B" som utdyper forhold omkring bruk av Digimarc.

Etter at jeg utarbeidet versjon 2-5 av denne rapporten, har jeg blitt gjort oppmerksom på at jeg ved en inkurie hadde utelatt tekst som omtaler fravær av Digimarc på den undersøkte CDen fra Sjødin. Dette er nå inntatt i rapporten, og er den eneste endringen fra versjon 2.5 bortsett fra oppdatering av datoer. Tilføyelsen er lagt inn på side 8.

Versjon 2.7: Fjernet et avsnitt på side 6, som er bedre og mer utfyllende dokumentert i Gisle Hannemyrs rapport. Fjernet klokkeslett på side 26 da dette er utilstrekkelig dokumentert av meg men fullt ut dokumentert med skjermdump i Hannemyrs rapport. Klokkeslettet er ikke signifikant for argumentet, datoen er.

Stein A. J. Møllerhaug

Telefon +47 977 37 830

e-post: mollerh@online.no

Rådgiver informasjonssikkerhet siden 1986, CISSP, CISSP Trainer
og ISO 27001 Lead Auditor trainer. Daglig leder Digital Truth ltd (NUF-UK)

Innhold

Mandat 2
Konklusjoner og oppsummering 2
Grunnprinsipper for digitale bevis 3
Bevisene 4
Fravær av dobbeltkontroller 5
Fravær av opplysninger om sletting/arkivering av materiale 6
Prosedyrefeil 7
Konsekvenser 8
Om Digimarc 8
Om "passordet" og dets pålitelighet 11
Tidsvindu 12
CDen utlevert til Sigurd Klomsæt 12
Forklaring av tidslinjen 13
Spesifikke kommentarer til tingrettens beslutning 15
Spesifikke kommentarer til lagmannsrettens kjennelse 16
Mulige scenarier 17
Vedlegg A Om Digitale vannmerker 18
Fjerning 18
Mangel på knytning samt gjenbruk 18
De konkrete bildene 19
"Terrorist i jern 1" 19
Uregistrert Digimarc 20
Digimarc og person 21
Vedlegg B Utfyllende kommentarer om elektroniske bevis 22
Innledning 22
Beviskjede (chain of custody) 22
Lekkasjesaken 23
Logging 23
Avsluttende merknader 24
Vedlegg C, tidslinjedata 26

MANDAT

Jeg ble den 27. mai 2012 engasjert av advokat Sigurd J. Klomsæt, som har gitt følgende mandat:

> *"Det legges ingen føringer i arbeidet/oppdraget – jeg vil ha sannheten og de faktiske korrekte forhold opp og fram – så langt det er mulig. Ditt arbeid står jeg fritt til å benytte overfor domstoler, politiet og andre organer".*

Mine kvalifikasjoner fremkommer i CV, som oppdragsgiver står fritt til å distribuere.

Sigurd Klomsæt har i denne saken fritatt meg for enhver taushetsplikt.

KONKLUSJONER OG OPPSUMMERING

Hovedkonklusjonene i denne rapporten er som følger:

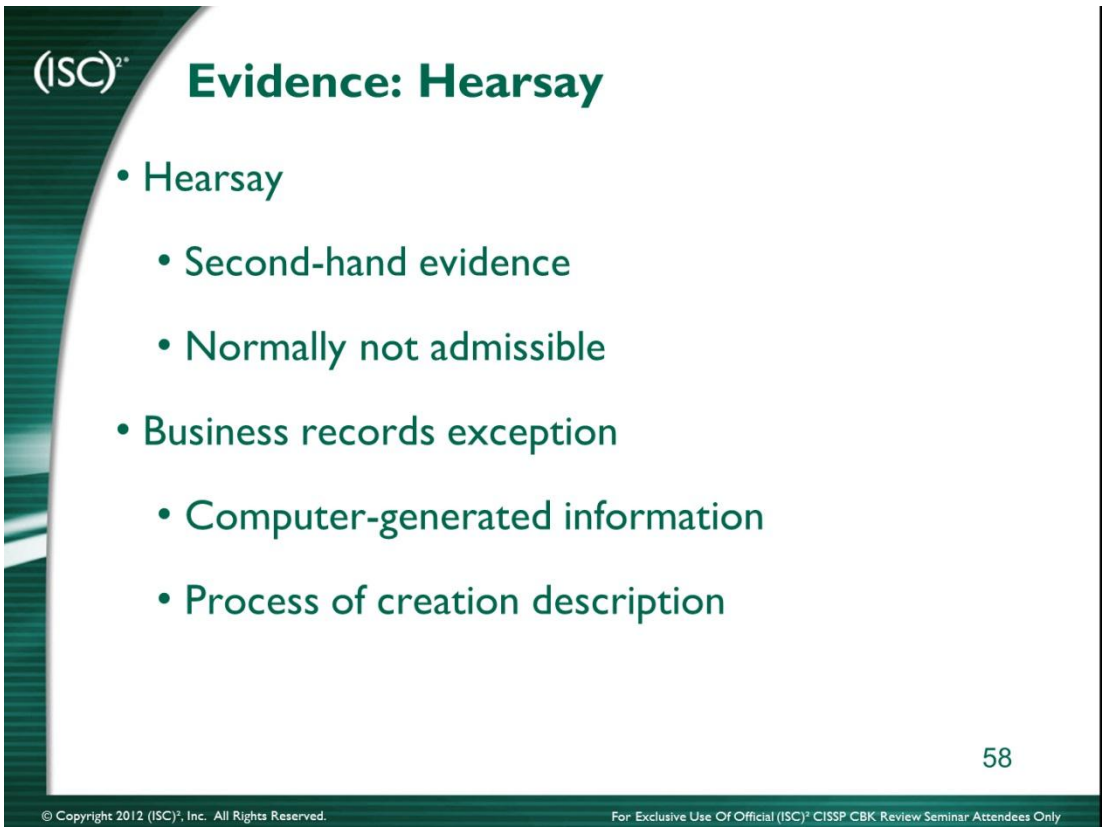
1. Politiet har i denne saken gjennomført en bevisinnsamling som strider mot selv grunnleggende prinsipper for elektronisk bevishåndtering, spesifikt:
    a. Beviskjeden er brutt
    b. Det foreligger ingen dobbeltkontroller
    c. Nøkkeldokumentasjon mangler
    d. Mulig frifinnende bevis er inndratt av politiet
    e. Det er benyttet en uegnet metode for digital vannmerking
2. Det er gjennom mine undersøkelser bevist at politiets beskrevne og påstått gjennomførte prosedyrer avviker fra de faktiske forhold på minst to meget kritiske punkter.
3. Begge rettsinstanser som har behandlet saken legger utelukkende politiets beviselig feilaktige påstander til grunn for sine kjennelser. Senere behandling refererer til slutningene fra Tingretten.
4. Politiet har benyttet utilstrekkelig styrke i beskyttelsesmekanismene for det utsendte materialet. Dette betyr at man ikke er avhengig av det såkalte passordet for å få tilgang til materialet.
5. Politiet, retten og Bevilgningsnemnda benytter termen "bilder fra Klomsæts CD". Ut fra fremlagt dokumentasjon og mangel på dokumentasjon er dette <u>ikke bevist</u>.
6. Bruk av demoversjon av Digimarc gjør at hvem som helst kan legge et hvilket som helst vannmerke inn på et hvilken som helst bilde. Lekkasjer kan ha skjedd på andre måter enn fra den fysiske CDen som ble generert til Klomsæt.
7. Fraværet av kvalitetskontroll samt det påviste fravær av Digimarc på Eldens CD gjør at det ikke kan utelukkes at det er generert mer enn en CD med det samme Digimarc som på Klomsæts CD.

Jeg vil redegjøre for de funn og vurderinger som ligger til grunn for mine konklusjoner. For klarhetens skyld refererer jeg også til lærebokpensum for innsamling, bevaring, analyse og presentasjon av digitale bevis. Jeg benytter pensumet til (ISC)2™ som referansemateriale. (ISC)2 er en av verdens mest anerkjente organisasjoner for å sertifisere sikkerhetskonsulenter. Deres CISSP eksamen anses som "gullstandarden" innen sikkerhetssertifisering.

Jeg er så vidt jeg vet den eneste nordmannen som er sertifisert til å undervise etter deres pensum, og en vesentlig del av mitt arbeid er å holde sertifiseringskurs over hele verden. Jeg holdt et kurs i Oslo i mars, i Helsingborg i april, i Warszawa i mai, i Dar El Salaam i juni, Dubai i juli og Johannesburg i august.

GRUNNPRINSIPPER FOR DIGITALE BEVIS

Innen fagområdet "digital forensics" lærer man hvilke informasjonskilder[1] som finnes på datasystemer, hvordan man sikrer informasjonen fra ulike informasjonsbærere, hvordan den analyseres og sammenstilles og hvordan informasjonen best kan presenteres.



Figur 1 Fra pensumet til (ISC)2 CISSP eksamen, digitale bevis' stilling i de fleste rettssystemer.

Alle datatekniske bevis er å betrakte som "formidlet informasjon fra tredje part" (datamaskinen) eller "hearsay". Dette stiller strenge krav til dokumentasjon og etterrettelighet.

[1] Informasjonskilder omtales ofte som data-bærere. Dette omfatter alle enheter som kan lagre informasjon som er lesbar for en datamaskin, slik som (men ikke begrenset til) CD plater, disketter, minnepinner, harddisker.

Et av nøkkelprinsippene for digitale bevis, er **etterprøvbarhet**. Dette betyr at to kompetente personer som uavhengig undersøker ektheten i digitale bevis, skal kunne finne de samme resultater når de undersøker det samme bevismaterialet.

Et annet grunnprinsipp er "logg alt, og så logger du at du logger".

Uten grundige rutiner for bevishåndtering, risikerer man i ytterste konsekvens å overføre den dømmende makt til tekniske eksperter gjennom deres nærmest ubegrensede muligheter for å underslå, endre, kopiere eller legge til materiale i en sak, enten dette skjer tilsiktet eller ved uhell.

I domspremissene i den gjeldende saken har man utelukkende vektlagt politiets forklaring og sett bort fra alle innvendinger reist av datasakkyndige samt vitneutsagn.

Det er reist en rekke innvendinger og det er av advokat Klomsæt og hans datakyndige Stuf as v/Geir-Otto Jakobsen krevet utlevert svært berettiget og supplerende dokumentasjon. Disse henvendelsene er møtt med taushet. Sentrale personer er ikke avhørt, og mulige alternative scenarier er ikke etterforsket.

Bevisene

Politiet la en felle for å identifisere hvem som lakk informasjon om 22. juli saken til pressen. Det ble benyttet to elementer: Et digitalt vannmerke ("Digimarc – Image" serienummer) og fjerning av noen mindre detaljer i det originale bildematerialet.

Politiet har redegjort for prosessen de har benyttet. Basert på politiets egen redegjørelse, er prosessen ikke etterrettelig. Jeg har fem hovedinnvendinger til prosessen:

1. Fravær av dokumentasjon av prosessen
2. Fravær av dobbeltkontroller i prosessen
3. Fravær av opplysninger om sletting/arkivering av generert materiale
4. Fravær av dokumentasjon av ubrutt beviskjede etter at CDene ble generert
5. Totalt fravær av merking av utleverte CDer.

Bildet viser en av de utleverte CDene som inneholder Utøya materiale. Begge CDene jeg har undersøkt ser like ut. CD boksen hadde heller ikke noen unike kjennemerker. Bildet er tatt på advokat Eldens kontor.

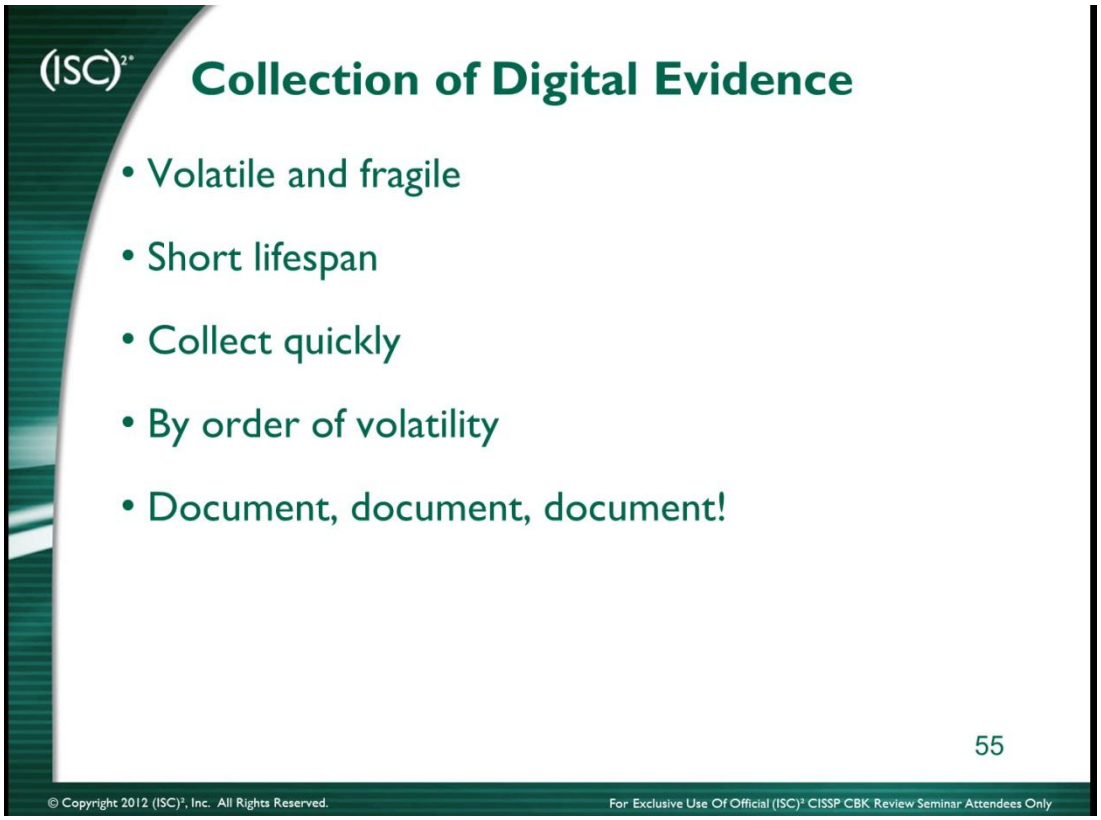
Politiets håndtering av denne saken fremstår som impulsiv, dårlig planlagt og dårlig gjennomført. Det mangler dokumentasjon, det kan ikke dokumenteres noen ubrutt beviskjede og det eksisterer ingen form for etterprøvbarhet i saken.

Uten etterprøvbarhet og med en brutt beviskjede, er digitalt materiale uegnet som bevis.

Bildemateriale fra saken var dessuten pressen i hende minst to dager før advokat Klomsæts kontor hadde fått utlevert materialet. Det er imidlertid uvisst hva dette

materialet inneholdt, men det er omtalt som "betydelig" og VG journalisten tok kontakt med bistandsadvokatene for å forberede de pårørende på publikasjon av materialet.

Dette beviser at det må være minst en lekkasjekilde i politiet.



Figur 2 Fra pensumet til (ISC)2 CISSP eksamen, hovedprinsipper for digital bevisinnsamling.

Fravær av dobbeltkontroller

Det er et grunnleggende sikkerhetsprinsipp at alle kritiske operasjoner skal være gjenstand for dobbeltkontroll. I dette tilfellet gjør politiet det til ***et sikkerhetstiltak at det ikke benyttes dobbeltkontroller***.

Dette er oppsiktsvekkende, og jeg (som andre datasikkerhetskyndige) skulle gjerne ha hørt en av de involverte politimennene foredra på en sikkerhetskonferanse og forsvare denne fremgangsmåten. Det er også oppsiktsvekkende at polititjenestemannen, i følge egen forklaring, heller ikke har orientert sine overordnede.

For å ha noen som helst grad av troverdighet, må en slik felle minimum ha to personer involvert som gjensidig kontrollerer hverandres arbeid. I tillegg må disse uavhengig av hverandre gjennomføre hver sin logging av alle aktiviteter i forbindelse med oppsettet av fellen og kvalitetskontrollere hverandres arbeid.

Mangelen på logging og dobbeltkontroll åpner for personlige uhells- eller fortsett-baserte feil hos den som produserer materialet. En slik feil kan for eksempel være at det produseres mer enn et dokumentasjonssett med det samme bilde-ID (Digimarc) eller slippes ut noen CDer uten Digimarc.

Slik prosessen er beskrevet av politiet, er alt prisgitt èn persons vurderinger og udokumenterte handlinger. Det kan sammenliknes med at èn enkelt

politibetjent er på fartskontroll hvor fartsmåleren svikter, men han velger likevel å bøtelegge og inndra førerkort basert på skjønn (øyemål) av farten.

Fravær av opplysninger om sletting/arkivering av materiale

Materialutleveringen består av et meget stort antall filer, både tekst, bilder og video. Arbeidet med å systematisere og samle dette må ha vært meget omfattende.

Et nøkkelspørsmål her er hvordan politiet kan dokumentere at ingen hadde tilgang til det benyttede datautstyret. Uten den informasjonen er politiets forklaring en interessant historie men uten noen som helst relevans for å plassere ansvar for lekkasjene hos Sigurd Klomsæt.

Jeg viser i denne sammenhengen til brev fra Advokatfirmaet Stabell & Co til Riksadvokatembetet, Oslo Statsadvokatembeter og Oslo Politidistrikt datert 3. februar 2012 om lekkasjer av billedmateriell til VG redaksjonen. I en e-post sendt fra journalist Morten S. Hopperstad i VG, 1. februar 2012 klokken 16:21, opplyser journalisten at de har billedmateriell, som det er opplyst (av anmelder) at bistandsadvokatene ikke har tilgang til. Denne henvendelsen skjer to dager før advokat Sigurd Klomsæt får tilgang til materialet han angivelig skal ha lekket. I tillegg finnes det vitneutsagn som indikerer at det mye omtalte "politiuniformbildet" har vært tilgjengelig på Internett fra desember 2011.

Jeg viser også til at bruken av uregistrert Digimarc gjør at om et bilde uten Digimarc ble tilgjengelig for uvedkommende og det var kunnskap om hvilke Digimarc som skulle benyttes, så kan det i løpet av sekunder legges inn et hvilket som helst Digimarc på bildet.

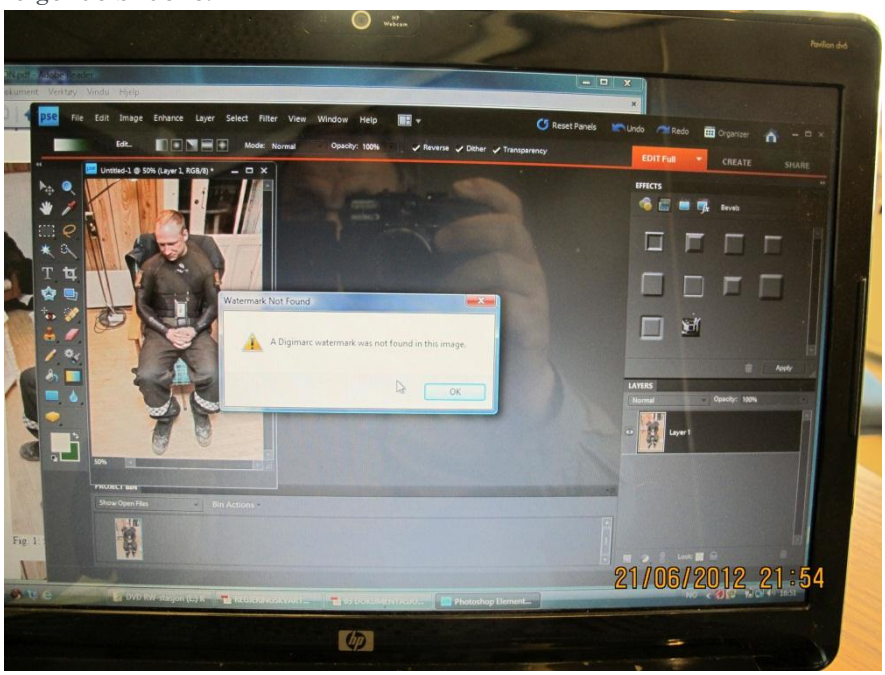
Det har tidligere skjedd lekkasjer av materiell som Klomsæt og de andre bistandsadvokatene ikke har hatt tilgang til. Dette må nødvendigvis skyldes interne politilekkasjer.

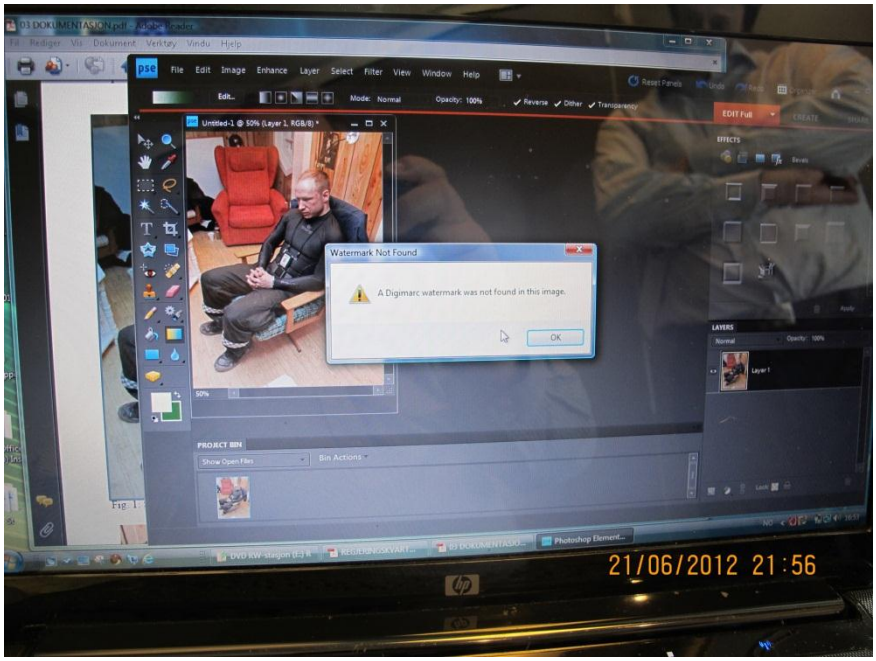
Vedkommende som har stått bak de tidligere lekkasjene har følgelig hatt en sterk motivasjon for å plassere denne lekkasjen utenfor politiet. Alt vedkommende ville trenge for å gjøre dette var kjennskap til at Digimarc skulle benyttes og ett enkelt "image-id". Hvilket "Image ID" som ble valgt benyttet kan og kan ikke ha vært en tilfeldighet.

I henhold til vitneutsagn fra politioverbetjent Hafredal, trodde politiet på dette tidspunktet at et Digimarc ikke lot seg fjerne uten et "betydelig kvalitetstap som ville være enkelt å se".

Prosedyrefeil

Ved gjennomgang av CDen utlevert til Advokat Elden, oppdaget jeg at de to aktuelle "uniformbildene" på denne CDen ikke hadde digitalt vannmerke. Jeg viser til de to følgende bildene:[2]





Dette er i strid hva politiet selv har forklart og uttalt til pressen. Det viser en klar prosedyrefeil.

[2] Kameraets klokkeslett er 5 timer feil, fotograferingen fant sted klokken 16:56. Merk at så vel rapportforfatter som advokat Elden er synlige i gjenskinn på skjermen.

Advokat Elden erklærer i en e-post:

```
Fra: "John Christian Elden" <j.c.elden@elden.no>
Til: <sigurd.klomsaet@klomsaet.no>
Emne:
Dato: fre., juni 22, 2012 09:03


På din anmodning bekrefter jeg at stein møllerhaug i går gikk
gjennom min cd mottatt ved politiets brev av 030212 og sjekket de to
aktuelle bilder i photoshop. Hans konklusjon var at det ikke var
noen form for vannmerking av bildene overhodet. Han viste meg funnet
sitt og fotograferte dette.

Sendt fra min HTC
```

Jeg har undersøkt Eldens og Sjødins CDer. En har vannmerke og en har ikke. Statistisk sett betyr dette at jeg hadde om lag 1/170 dels sjanse for å finne en CD uten Digimarc dersom det kun var begått en enkelt prosedyrefeil. Det gjør det overveldende sannsynlig at det er begått betydelig mer enn en feil i genereringen av materialet.

I tillegg har jeg lett i de tre CDene jeg etter hvert har fått tilgang til etter et Digimarc i videoen som skulle merkes med Digimarc. Jeg finner ikke Digimarc i noen av videoene, noe som dokumenterer ytterligere et avvik fra prosedyren politioverbetjent Hafredal har redegjort for at skulle følges.

Konsekvenser

Selv tilstedeværelse av en enkelt CD produsert gjennom feil prosedyre er kritisk for materialets beviskraft, da dette dokumenterer prosedyrefeil. Det må derfor stilles kritisk spørsmål med hele politiets håndtering av materialet.

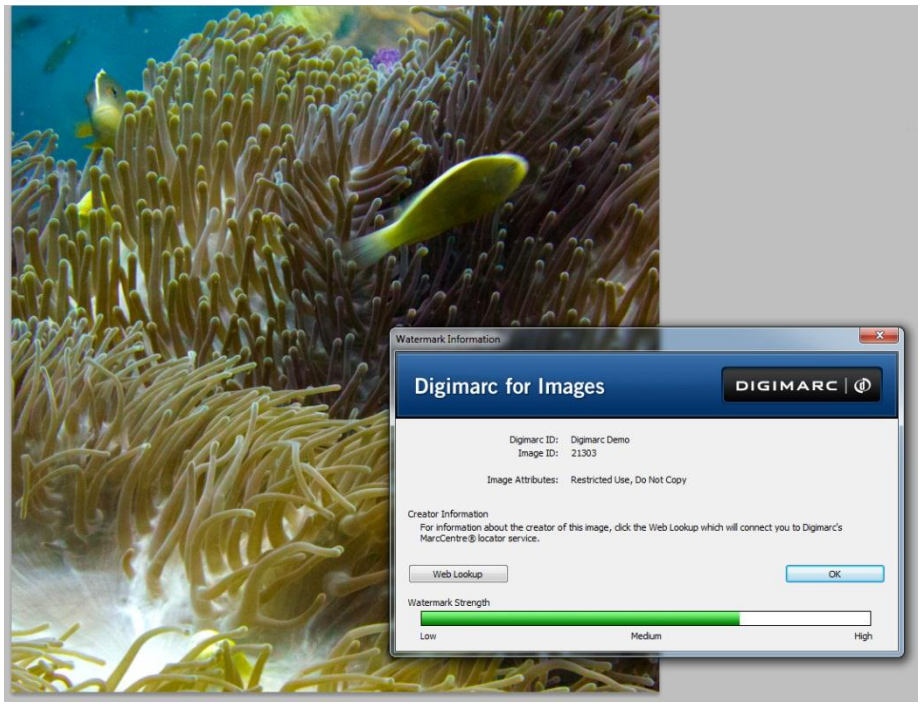
Slik beviset foreligger nå, er det i samme klasse som forurenset DNA materiale.

Om Digimarc

Bruk av Digimarc fremholdes som noe ufeilbarlig og autoritativt.

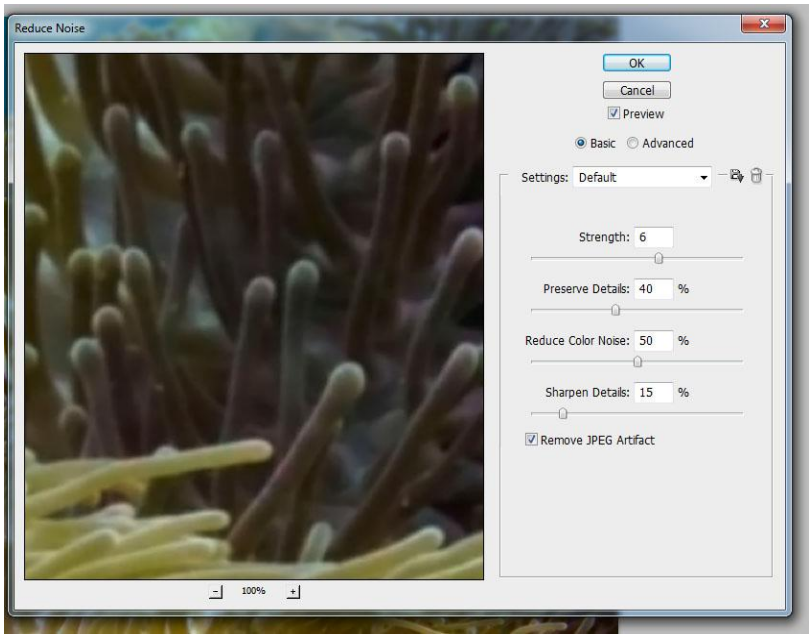
Jeg har tatt et dykkerbilde og påført dette "Digimarc Image ID" 21303 med "Digimarc ID" 10101 (som vises som "Digimarc Demo"). I følge politiets bevislogikk må dette bildet stamme fra "CDen utlevert til advokat Klomsæt"!

Her benytter jeg politiets egne faglige argumentasjon i forhold til styrken på Digimarc. De påstår at dersom et bilde har Digimarc 21303 så må dette stamme fra CDen som ble utlevert til Sigurd Klomsæt.



Figur 3 Dette bildet har et Digimarc, usynlig for det blotte øyet. Nummeret er 21303, det samme nummeret som politiet hevder er benyttet på utvalgte bilder i utleveringen til bistandsadvokat Sigurd Klomsæt. "Watermark Strength" er høy fordi bildet har mange detaljer, hvilket gjør skjulingen av (det for det blotte øyet usynlige) vannmerket enklere.

Jeg har eksperimentert med Photoshop og Digimarc og kan konstantere at politiets utsagn er rent vrøvl. For å fjerne Digimarc, må man bruke en "gaussian blur" med en setting på minst 6,2. ***En slik "blurring" vil fullstendig ødelegge bildet.*** Bruker man derimot "reduce noise" filteret, får man ikke det samme kvalitetstapet og Digimarc dataene (vannmerket) blir likevel fjernet.



Figur 4 Innstillingene jeg benyttet for å fjerne Digimarc fra eksempelbildet.

Etter noen minutters eksperimentering, fant jeg disse innstillingene som helt fjernet det eksisterende Digimarc fra bildet. Resultatet kan sees i neste illustrasjon.

En fotografkyndig vil kunne finne noen minimale forskjeller mellom de to bildene, men forskjellene vil ikke kunne sees i bilder som er gjengitt i oppløsning passende for web-sider.

Vær også oppmerksom på at min fjerning av Digimarc var et enkelt eksperiment. Jeg stoppet når vannmerket ble borte. Etter dette eksperimentet har jeg raffinert innstillingene og lykkes å fjerne Digimarc med langt mer moderate innstillinger og følgelig enda mindre kvalitetstap.

Etter å ha fjernet Digimarc fra bildet, kunne jeg så enkelt legge inn et nytt Digimarc, med den verdien jeg selv bestemte, for eksempel 21304 som vil være Digimarc Image ID for en annen bistandsadvokat. Digimarc gir følgelig ingen sikkerhet mot forsettlig manipulasjon (fjerning og endring) når funksjonen blir brukt som uregistrert (DEMO) bruker slik politiet gjorde.

Hvem som helst kan legge inn et hvilket som helst Digimarc i bildene. Alt som kreves er tilgang til bildene og kjennskap til hvordan "Image ID" ble valgt.

Digimarc File Id 21303

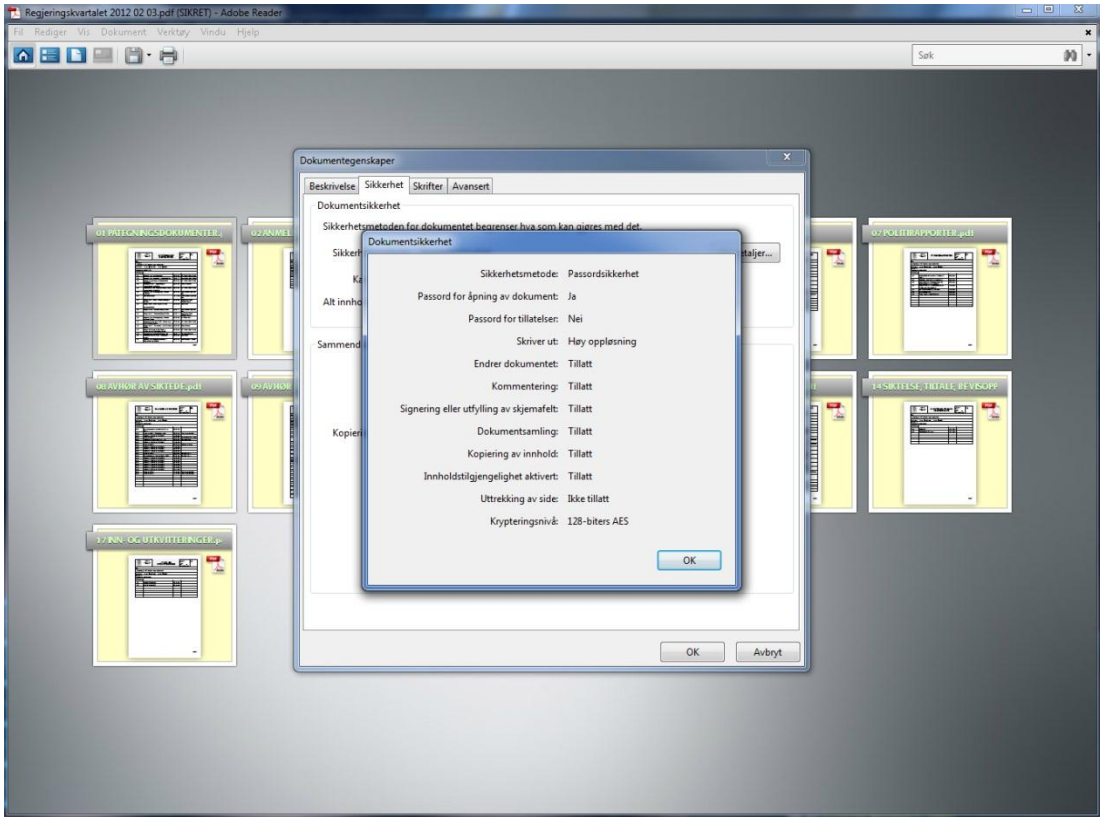
Samme bilde, men Digimarc informasjon er fjernet ved hjelp av REDUCE NOISE

Figur 5 Resultatet etter å ha kjørt "Reduce noise" med settingene fra figur 4. Bildene er tilgjengelige i større versjoner.

Det vises til "Vedlegg B" for utdypende kommentarer om Digimarc.

OM "PASSORDET[3]" OG DETS PÅLITELIGHET

Det gjøres et meget stort nummer av at CDenes innhold var "passordbeskyttet".



Bildet viser sikkerhetsdata fra Arvid Sjødins eksemplar. Det fremgår at den sterke AES-128 krypteringsalgoritmen (Advanced Encryption Standard) er benyttet. Dette skal i teorien gi god sikkerhet mot "passordknekking" – men slik sikkerhet betinger et passord som er lengere enn 8 tegn. Sjødin har et 10 tegns passord, men passordet som ble utlevert til Sigurd Klomsæts kontor var på kun 8 tegn

Det finnes både nedlastbare gratis og kommersielle programmer på nettet som knekker 8 bokstavers PDF passord basert på AES. Sikkerhetsspesialister vet at mens passord kompleksitet (blanding av tall, små bokstaver, store bokstaver og spesialtegn) hjelper til med å styrke passordet, så er den mest utslagsgivende faktoren passordets lengde.

AES er hva vi kaller en BLOCK CIPHER. Riktig brukt anses AES-128 for å være sikker. Feil brukt kan algoritmen svekkes sterkt og bli uegnet til beskyttelse.

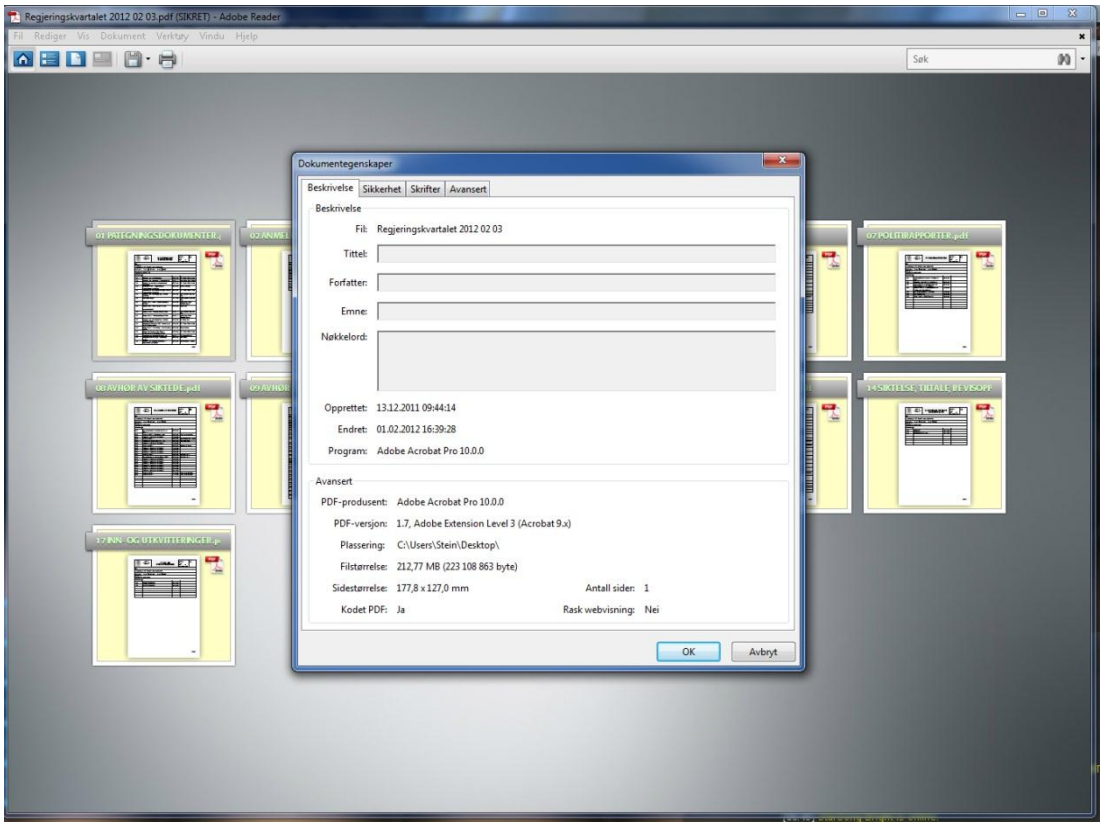
Et passord på 8 tegn (bytes) utgjør en krypteringsnøkkel på 64 bits. Det er benyttet AES-128 som er basert på en nøkkel på 16 tegn (128 bits). Bruk av kortere nøkler svekker algoritmen, da krypterings-systemet han ikke selv "finne på" de manglende tegnene. Algoritmen kan følgelig aldri bli sikrere enn den nøkkelen som benyttes.

Etablering av dette passordet og håndtering av det er dessuten ikke dokumentert. Kjennskap til eller mangel på kjennskap til passordet har derfor ingen beviskraft og er i beste fall et svakt indisium. Dette er relevant dersom lekkasjen har skjedd som en følge

[3] Det såkalte passordet er ikke egentlig et passord slik det benyttes her men en krypteringsnøkkel (kodenøkkel). Jeg benytter derfor anførselstegn når jeg refererer til begrepet "passord".

av at selve CDen som ble utlevert eller en kopi av denne oppbevart hos politiet kilden til lekkasjen.

TIDSVINDU



Metadata fra Sjødins CD (over) viser at filen som inneholdt hans utsendelse første gang ble opprettet 13.12.2011 klokken 09:33:14. Den er siste gang endret 01.02.2012 klokken 16:39:28.

CDen utlevert til Sigurd Klomsæt

Politiet har beslaglagt den opprinnelige CDen som ble utlevert til Sigurd Klomsæt. Derved ville de normalt ha fratatt ham en av mulighetene til å bevise uskyld. Før beslaget skjedde var det blitt tatt en full image kopi (ISO-image) av CDen av Sigurd Klomsæts data-ansvarlige. Jeg har mottatt en kopi av denne ISO imagen. Jeg kan redegjøre for en ubrutt beviskjede for denne fra Klomsæts dataansvarlige. Han kan redegjøre for en ubrutt beviskjede fra den ble kopiert.

CDen er åpnet ved bruk av passordet som ble gitt til Sigurd Klomsæt.

Basert på undersøkelse av metadata fra min kopi av "Klomsæts CD", har jeg lykkes å konstruere en delvis komplett tidslinje for produksjon av CD platen. Jeg har sammenliknet opprettelsesdatoer og siste revisjonsdato mot Sjødins CD.

De fleste filene har samme opprettelsesdato og dato for siste revisjon unntatt:

1. Masterdokumentet (containerfilen) som er filen som samler alle underdokumentene og gir disse kryptografisk beskyttelse.
2. "03 Dokumentasjon" – som inneholder de bildene som ble påført Digimarc
3. "07 Politirapporter" – som i følge politiets beskrivelser ikke skal være modifisert, hvilket beviser nok ett avvik fra prosedyren politiet beskriver.
4. "08 Avhør av siktede" - som i følge politiets beskrivelser ikke skal være modifisert, hvilket beviser nok ett avvik fra prosedyren politiet beskriver.

Det er tidligere gitt inntrykk av at politiet hadde full kontroll innen et snevert tidsvindu i forbindelse med produksjon av CDene. Det snevre tidsvinduet har vært benyttet til å begrunne at data ikke kan ha lekket. Her vises det at "lekkasjevinduet" på 10 dager nær har vært på hele 2 måneder og ikke "noen timer" slik tidligere fra politioverbetjent Hafredal..

Sigurd Klomsæts CD ble i følge data hentet fra kopien av CDen hans laget allerede mandag 30. januar 2012 klokken 20:19:33. Dette betyr at den har foreligget i "ferdig form" i nesten 4 døgn før den første eksponeringen av bildemateriell og står i kontrast til Arvid Sjødins CD som ble gjort ferdig først 01. februar 2012 klokken 16:39:35.

Dette gir et betydelig vindu for lekkasje. I kombinasjon med bruk av kun 8 tegn i "passordet" gir dette mange ganger mer tid til disposisjon enn det som er påkrevet for å la et dataprogram prøve ut alle mulige passordkombinasjoner.

Etter som Arvid Sjødins CD først ble ferdigstilt 01. februar 2012 klokken 16:39:35 og har 10 tegns "passord", ville det ikke latt seg gjøre å knekke passordet for denne ved å prøve ut alle mulige passordkombinasjoner i tiden fra ferdigstillelse av CD til publisering. Dette skyldes at det for hvert tegn som legges til et "passord", blir arbeidsmengden med å prøve ut alle mulige kombinasjoner doblet.

Tidlig produksjon av Klomsæts CD i kombinasjon med et kort "passord" er derfor særdeles uheldig i forhold til risiko for kompromittering av den ferdige CDen.

Forklaring av tidslinjen

Jeg har laget en tidslinje for å anskueliggjøre de endringer som lar seg kartlegge. Datafiler for tidslinjen er vedlagt som vedlegg C.

I denne tidslinjen benyttes følgende fargekoder:

1. RØD – Viser tidsintervallet mellom opprettelse av filen og filens siste revisjonsdato.
2. GRÅ viser tidsintervallet fra siste revisjonsdato frem til publisering av bildene på nettavisene.
3. BLÅ viser tidsintervallet hvor det kan ha blitt laget en kopi av den ferdige CDen.

Dataene er relevante dersom lekkasjen har skjedd som følge av at noen har kopiert hele CDen. En slik kopiering er ett av flere mulige scenarier.

Etter som politiet i følge bekreftelse fra politioverbetjent Hafredal til advokat Arvid Sjødin er ute av stand til å redegjøre for hvilke endringer som skjedde når med materialet som utgjør beviset, kan lekkasje ha skjedd når som helst i "rød og grå" sone.

Det er heller ikke redegjort for når masterfilen ble kryptert med Klomsæts 8 tegns "passord", men dette sammenfaller trolig med siste tidspunkt for revisjon, hvilket for Klomsæts CD plasserer dette til 30. januar 2012 klokken 20:19:33. Dette betyr i så fall at masterfilen har vært ubeskyttet av kryptering fra 13. desember 2011 09:44:14 da den opprettes (samme fil for alle advokater) og man begynner å legge filer inn i masterfilen.

Kombinert med den påviste rutinesvikten må det stilles kritiske og alvorlige spørsmål med hele prosessen politiet har gjennomført i denne saken. Materialet som politiet har presentert er ikke bevis, men løse påstander fra en enkeltperson, påstander som direkte motsies av tekniske funn i saken.

SPESIFIKKE KOMMENTARER TIL TINGRETTENS BESLUTNING

"Retten er etter en samlet vurdering av alt fremlagt materiale overbevist om at de publiserte bildene stammer fra den CDen som denne fredagen av politiet ble utlevert advokat Klomsæts sekretær i henhold til fullmakt fra Klomsæt."

Premisset for slutningen er feil. Det er ingen ting som beviser at de fremlagte bildene stammer fra den CDen som ble utlevert til Klomsæts kontor. Ref blant annet Gisle Hannemyrs uttalelser.

Hva som er bevist er at bildene som ble publisert hadde samme Digimarc bilde ID (21303) som de bildene som ble lagt på CDen som ble utlevert Klomsæts kontor. Men det har dykkebildet mitt også.

"Politiet har opplyst at hver enkelt CD kan kopieres på vanlig måte, men at en slik kopi bare kan åpnes med bruk av det tilhørende unike passordet. Kopiering av denne datamengden til minnepinne tar omkring to minutter".

Premisset for slutningen er feil. Det er benyttet PDF kryptering (AES-128) med usikker nøkkellengde.

Bruk av kryptering gir ingen reell beviskraft uten et skikkelig system for nøkkeladministrasjon. Bruk av kort krypteringsnøkkel (8 tegn) gir ytterligere svekking av den allerede ikke-eksisterende beviskraften.

"At CDer skulle utleveres denne dagen..." (avsnitt forkortet)

Slutningen er en ren spekulasjon som ikke er støttet av noe fremlagt bevis. Dersom forutsetningene bortfaller, bortfaller også hele denne slutningen.

"Lekkasjer fra andre i politiet som ikke er en del av 22. juli teamets utvalgte kan i denne sammenhengen utelukkes fordi ingen slike har hatt tilgang til disse konkrete CDene og ingen har hatt tilgang til passordene. Det er bare en person som hadde tilgang til begge deler."

Premissene for slutningen er feil. Det er dokumentert prosedyrefeil. Det er ikke dokumentert noen ubrutt beviskjede. Det er ikke fremlagt noen loggingsinformasjon for prosesseringen. Det er ikke noe behov for tilgang til passordene for å få tilgang til PDF filen. Og det benyttede Digimarc er ikke knyttet til Klomsæt eller noen ved hans kontor. Det er trivielt å fjerne og endre et Digimarc. Og det er vist lekkasjer til pressen før Klomsæt får tilgang til sin CD.

Lekkasjer fra politiet, 22. juli teamet, ansatte i Politiets Data og Materielltjeneste, vaskepersonale, teknikere eller andre kan på grunn av brutt beviskjede ikke utelukkes.

SPESIFIKKE KOMMENTARER TIL LAGMANNSRETTENS KJENNELSE

"Lagmannsretten legger til grunn at de bildene som ble publisert i forskjellige nettaviser senere samme ettermiddag, inneholdt de unike bilde-iD-ene som var lagt inn på den CDen som ble utlevert advokat Klomsæts sekretær, Lisbeth Freang Klomsæt."

Her treffer Lagmannsretten bedre enn Tingretten i sin beskrivelse av hva som er tilfelle: Nemlig at bilder med samme bilde ID dukker opp på nettet. Men utsagnet er likevel feil, fordi begrepet *"unike bilde-iD-ene"* benyttes. Digimarc i DEMO modus gir ingen *"unike iD-er"*, er aldri laget for å gjøre det og er ikke ansett som noe pålitelig sikkerhetstiltak for unikt å identifisere et bilde.

"Advokat Klomsæt har anført at sikkerhetsløsningen kan knekkes. Det forutsetter imidlertid at man har den fysiske CDen."

Dette er feil. Man kan også knekke sikkerhetsløsningen om man har en kopi av CDen. Det er ikke vist noen ubrutt beviskjede her. Videre er ikke knekking av sikkerhetsløsningen påkrevd dersom CDens innhold allerede er lekket. Da trenger man kun å endre Digimarc for å gi Klomsæt skylden for lekkasjen.

"Lagmannsretten ser også bort fra den forklaring som er gitt fra advokat Klomsæt om at et slikt iD-merke kan fjernes, og at det kan legges inn en ny iD på bildet. Det vises til politiets redegjørelse om at det vil føre til at bildet blir uskarpt. Det var ikke tilfelle her og lagmannsretten bemerker at dette kan konstateres ved selvsyn ved de fremlagte dokumenter. De bilder som er publisert i pressen er like skarpe som de opprinnelige bildene."

Dette er direkte feil, jeg viser til min utredning og dokumentasjon over om hvordan Digimarc kan fjernes uten synlig kvalitetstap.

"Advokat Klomsæt har også indikert at noen kan ha sørget for at CDene kom på avveie for å skade ham. Lagmannsretten viser her til tingrettens redegjørelse nederst side 5 og øverst side 6 som lagmannsretten slutter seg til. Også lagmannsretten finner det utelukket at politiet selv har sørget for å videreformidle materialet til pressen for å ramme Klomsæt som advokat. Det vises for så vidt til det faktum lagmannsretten bygger på som beskrevet ovenfor. Tjenestemennenes fremgangsmåte var valgt nettopp for å utelukke lekkasjer fra politiets egne datanettverk. Det er også svært lite sannsynlig at noen på en eller annen måte har blitt kjent med hvilken PC det sensitive materialet har ligget på de aktuelle dagene og hacket seg inn på den for så å sende dette til pressen."

Dette er det intet grunnlag for å fastslå, og dette dekker bare ett av flere mulige scenarier. Politiets rutiner oppfattes som grundige mens faktiske funn i saken viser det motsatte. Ved at kun èn person er ansvarlig for sikringen, fratas dessuten muligheten til etterprøvbarhet og kvalitetskontroll og man åpner muligheten for personlige feil av den typen som er funnet med det manglende Digimarc.

"Videre er det anført at det er på det rene at det ikke er sendt epost som inneholder noe om CDen fra noen av datamaskinene på advokat Klomsæts kontor. Lagmannsretten vil bemerke at denne CDen kan ha blitt kopiert til en annen CD eller en minnepinne og at dette kan gjøres meget raskt. Tilgang til den kopierte CDen vil man imidlertid ikke kunne få uten å ha tilgang til passordet."

Dette er en ren spekulasjon. Den gjøres verre ved at det uriktige utsagnet om at man trenger tilgang til passordet for å kunne lese CDens innhold gjentas.

"Ut fra de forklaringer som er gitt av advokat Klomsæt og advokatfullmektigen, har både fullmektigen og advokat Klomsæts sekretærer hatt tilgang til CDen. Det er ikke på det rene hvem, ut over advokat Klomsæt og fullmektigen, som har hatt tilgang til passordet."

Igjen legges forutsetningen om at tilgang til CDens innhold krever tilgang til passordet. En uriktighet, endog usannhet, blir ikke mer korrekt hhv sann fordi om den gjentas.

Videre premisser er basert på gjentakelse av og spekulasjon basert på de allerede tilbakeviste påstander. Lagmannsrettens slutninger er derfor ikke i tråd med fakta i bevismaterialet. Det er ikke kjent at tingretten eller lagmannsretten har gjort egne undersøkelser.

MULIGE SCENARIER

Ut fra informasjonen i Lagmannsrettsaken, med fratrekk av de påstander som allerede er tilbakevist på teknisk grunnlag, fremstår det fire like mulige scenarier, som hverken er bekreftet eller avkreftet. Dersom skikkelige rutiner for håndtering av elektroniske bevis var blitt fulgt, ville trolig ett eller to av scenariene kunne ha blitt eliminert:

1. Lekkasjen har skjedd ved at noen ved advokat Klomsæts kontor har laget en kopi av CDen til pressen. Merk at det ikke var noe behov for å gi pressen passordet til CDen. De fleste redaksjoner har journalister som kan google "PDF password cracking".
2. Noen i politiet har bevisst lekket CDen med Klomsæts Digimarc eller en kopi av denne til pressen. Igjen er det ikke noe behov for å lekke passordet. Alternativt kan de samme aktører ha lagt Klomsæts Digimarc inn i materialet som lekkes til pressen, enten ved en tilfeldighet eller for å ramme Klomsæt.
3. Det begås en personlig feil under generering av CDene og mer enn en CD får det vannmerket som er registrert på Klomsæt. Denne aktøren står så bak lekkasjen.
4. Pressen mottar bilder med et Digimarc "Image ID", retter dette for å beskytte sin kilde og velger tilfeldigvis det "Image ID" som er tilordnet Sigurd Klomsæt.

Når Lagmannsretten kategorisk fastslår at Klomsæt står bak lekkasjen, har dette ikke noe fundament i fremlagte bevis. Hadde normal praksis for generering og sikring av elektroniske bevis (dokumentasjon, dualitet for kritiske operasjoner, ubrutt beviskjede og bruk av digitale signaturer) blitt fulgt, kunne man både ha kartlagt hva som skjedde og hvem som stod bak.

Oslo 02/11-2012

Stein A. J. Møllerhaug
CISSP, Certified CISSP Trainer,
Certified ISO 27001 Lead Auditor Trainer
Rådgiver og Daglig Leder Digital Truth ltd

VEDLEGG A OM DIGITALE VANNMERKER

Det eksisterer flere teknikker for å påføre bilder, tekst, stemmeopptak og videoopptak unike merker som identifiserer materialets opphav. I denne saken dreier det meste seg om en implementasjon av digitale vannmerker som heter Digimarc, utviklet av Adobe Systems Incorporated.

Adobe går svært langt på sine websider i å utrope Digimarc til den "endelige løsningen" på alle copyright problemer. Men selv ikke Adobe kaller Digimarc for "bevis". Realitetene er at digimarc merkingen er et nyttig hjelpemiddel som dessverre er beheftet med noen svakheter. I tillegg innfører politiet selv ytterligere en svakhet i måten de velger å utnytte Digimarc på. Svakhetene i systemet består i:

1. Merkene kan gå tapt i redigeringsoperasjoner.
2. Merkene er ikke uløselig knyttet til objektet som merkes.
3. Det samme merket kan brukes om igjen så mange ganger man ønsker.
4. Politiet har ikke registrert seg med noe Digimarc ID.

Jeg skal utdype de enkelte punktene i de påfølgende kapitler.

FJERNING

Politiet påstår at et påført Digimarc ikke kan fjernes uten et betydelig kvalitetstap. Dette er feil, det er vist i min første rapport samt i eksempelbilder i denne oppsummeringen. I eksempelbildene har jeg med vilje ikke gjort noen avansert redigering men holdt meg til en "to-museklikks" operasjon (Klikk FILTER – velg NOISE – velg REDUCE NOISE og klikk OK). Innstillingene som er benyttet er vist i bildematerialet. Samlet redigeringstid er under 5 sekunder.

I eksempelbildene er det ved nærmere granskning mulig å se minimale forskjeller mellom bildet med Digimarc og bildet uten, men det er ingen "betydelig kvalitetsreduksjon" slik hevdet av retten og av politiet.

Den lille kvalitetsreduksjonen som kan observeres, kan dessuten fjernes ved bruk av en enkel tilleggs-operasjon. I områder hvor "REDUCE NOICE" tar bort detaljer av betydning for bildet, kan man ved enkel maskeringsteknikk gjenopprette disse detaljene i de fleste redigeringsverktøy. Vede å øke fargemetning, endre svart-punkt, justere kontrast og tone, kan det redigerte bildet oppfattes som "bedre" enn det uredigerte bildet med Digimarc.

Digimarc lar seg fjerne fra et bilde uten synlig kvalitetstap.

MANGEL PÅ KNYTNING SAMT GJENBRUK

Det er brukeren (rettighetshaveren) av et bilde som bestemmer hvilket Digimarc et gitt bilde skal ha. Følgelig kan mer enn ett bilde ha det samme "Image ID", og ulike versjoner av ett bilde kan ha ulike Digimarc.

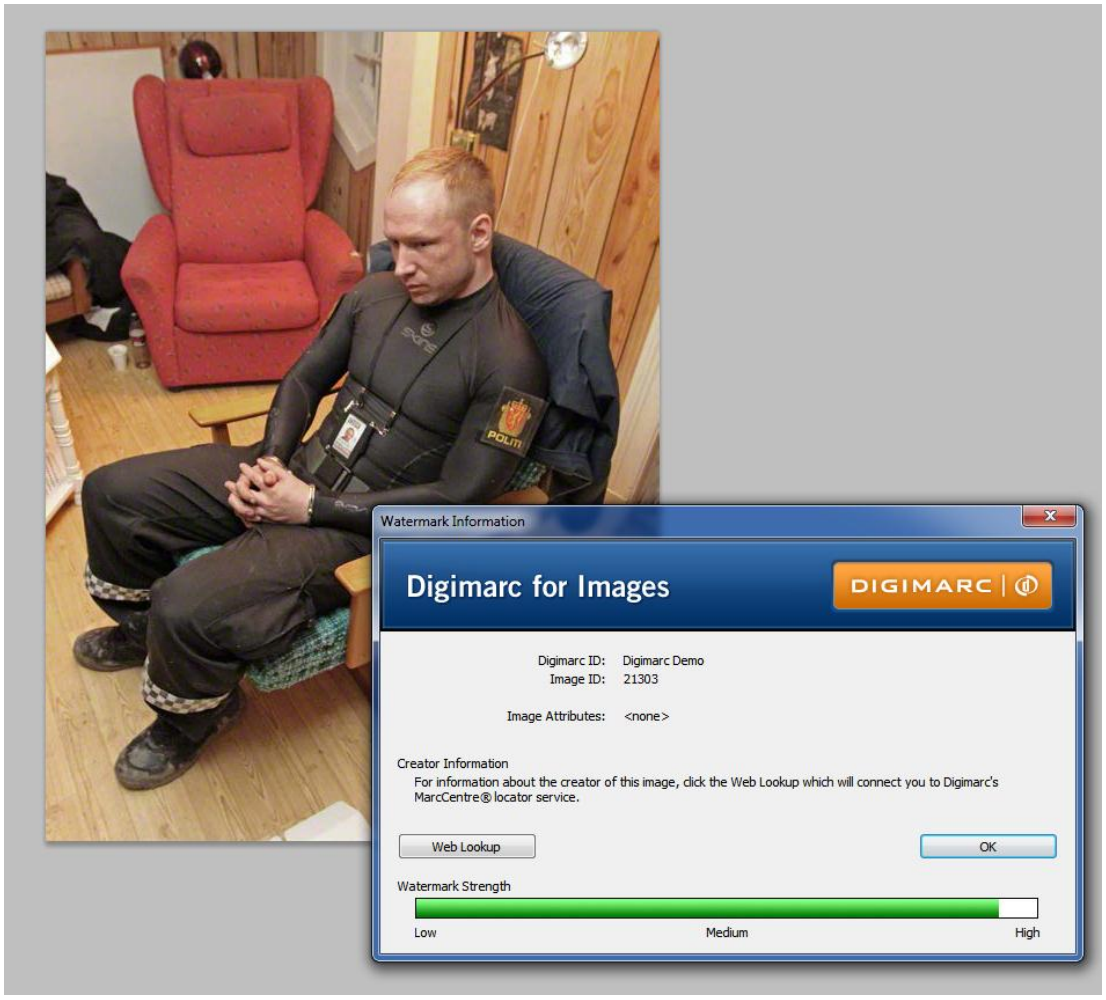
Dersom man fjerner et Digimarc fra et bilde, kan det lett legges inn et nytt "image ID", med de verdiene som innleggeren selv bestemmer.

Et Digimarc ID er derfor ikke uløselig knyttet til ett objekt, men kan gjenbrukes et ubegrenset antall ganger. Image ID kan fjernes og erstattes med et nytt.

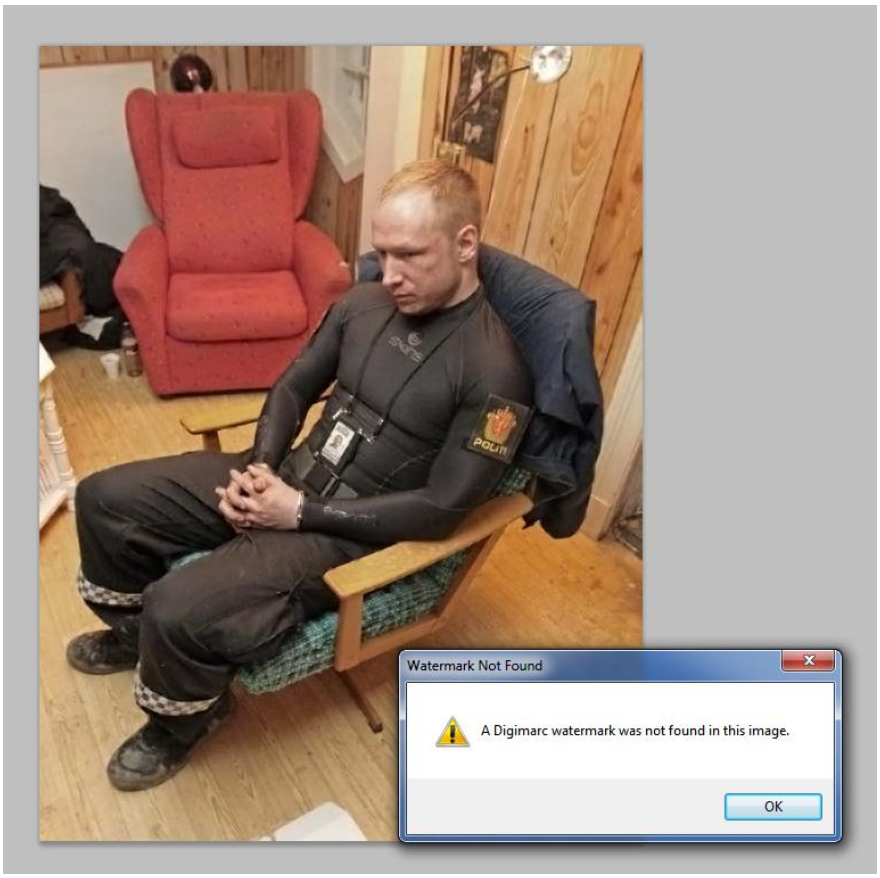
DE KONKRETE BILDENE

Nedenfor stående bilde viser ett av "ABB-bildene" med "Digimarc Image ID" 21303 som er det det samme "Image ID" som politiet tilordnet bildet på den CDen som ble utlevert til advokat Sigurd Klomsæt.

"Terrorist i jern 1"



Bildet er gjengitt i en størrelse som er om trent 1,5 ganger større enn det som ville være normalt for et bilde med denne oppløsningen. Dette fysiske bildet er en kopi av et bilde fra den CDen som ble utlevert til Sigurd Klomsæts. Bildet er fremskaffet ved å velge bildet, velge KOPIER og så lime bildet inn i Adobe Photoshop CS versjon 5.1.



I bildet ovenfor, har jeg fjernet Digimarc på enklest mulig måte (Klikk Filter – Reduce Noise – OK), med andre ord en tre-museklikks operasjon som tar under 5 sekunder. Et trenet øye kan se noen små forskjeller. Disse forskjellene kan lett fjernes med ytterligere bearbeiding, noe som tar mindre enn to minutter. De færreste vil påstå at det er en "betydelig kvalitetsforskjell" mellom de to bildene. Begge bildene er skalert slik at selve bildet av Brevik er like stort.

Jeg har tidligere vist hvordan jeg så kan legge inn et vilkårlig Digimarc i et bilde ved å legge inn Sigurd Klomsæts tilordnede "Image-ID" 21303 i et dykkerbilde.

Pressen er vel kjent med Digimarc, hvilke muligheter systemet gir og hvilke svakheter det er beheftet med. De fleste som jobber med bilder i pressen sjekker rutinemessig for tilstedeværelsen av Digimarc, da dette kan ha stor betydning med tanke på opphavsrett og royalties. Dersom pressen mottok et bilde med for eksempel Digimarc 21301 (nummeret er tilfeldig valgt) og ønsket å skjule sin kilde, hadde det derfor vært svært lett for dem å "rette" "Image ID" til et annet nummer, for eksempel 21303. Det ville ikke være logisk for dem å anta at politiet brukte sekvensiell tilordning av Digimarc. Når politiet likevel gjør dette, "planter" dette derved bildet uriktig hos Sigurd Klomsæt.

Uregistrert Digimarc

Digimarc softwaren fungerer med og uten registrering. Hvert Digimarc inneholder to elementer: Et "Digimarc ID" og et "Image ID". Det er kun sistnevnte som er benyttet i denne saken.

Adobe har bygget støtte for Digimarc inn i de fleste av sine produkter. I tillegg tilbyr de en tjeneste som tillater brukerne å registrere seg slik at de kan følge med hvor på nettet deres bilder befinner seg ved at de som registrerer seg, får de et unikt "Digimarc ID" og tilgang til en søketjeneste. Da er det kun den som eier denne ID-en som kan påføre den som Digimarc på materiale som skal beskyttes.

Dersom man ikke registrer seg (det er en kostnad med å registrere seg), kan man fremdeles påføre sitt materiale en "image ID", men alle som er uregistrerte vil ha "Digimarc ID" satt til "Digimarc Demo", nummer 10101. Det er dette politiet har gjort.

Hadde de registrert seg, ville de ha vært i stand til å påføre bildene en unik "Digimarc ID" som sammen med "Image ID" ville ha gitt en betydelig høyere sikkerhet enn hva de valgte, da "Image ID" og "Digimarc ID" begge ville ha kommet opp i bildet.

Det er mulig men langt fra enkelt å plassere en falsk "Digimarc ID" i et bilde. Det er trivielt å plassere et falsk Image ID i et bilde når det benyttes en uregistrert Digimarc bruker.

DIGIMARC OG PERSON

Uregistrert Digimarc er uegnet til å knytte sammen person og beskyttet materiale. Jeg ser i en rekke politiutredninger at de benytter begrepet "Bilder fra Klomsæts CD". Bruk av denne betegnelsen, for eksempel i utarbeidelse av tidslinje, konkluderer med at kilden er Sigurd Klomsæt, mens hele hensikten med bevisfremleggingen er å bevise dette. Slik bruk av konkluderende betegnelser i del-bevis er i beste fall uprofesjonelt.

Den korrekte betegnelsen fra politiets side ville være "Bilder med samme Digimarc Image ID som bildene vi la ut på Klomsæts CD". Deretter ville ytterligere bevisfremleggelse (journaler, logger, detaljredegjørelser, prosedyrebeskrivelser) eventuelt kunne ha blitt benyttet til å underbygge en konklusjon om at bildene faktisk stammer fra Klomsæts CD.

Slik saken står i dag er det bevist at bilder med Digimarc 21303 dukket opp i pressen kort tid etter at Sigurd Klomsæts sekretær mottok disse samt passordet til CDen på e-post. Det er ikke bevist at disse to begivenhetene er knyttet sammen. Det er følgelig heller ikke bevist at bildene stammer fra Klomsæts CD, og en lekkasje av bildene innenfor politiet kan heller ikke utelukkes.

Ettersom det ikke er bevist at bildene stammer fra den samme fysiske CDen som Klomsæts sekretær fikk utlevert, så er det heller ikke bevist at Sigurd Klomsæt eller noen ved hans kontor står bak lekkasjen.

Oslo 02/11-2012

Stein A. J. Møllerhaug
CISSP, Certified CISSP Trainer,
Certified ISO 27001 Lead Auditor Trainer
Rådgiver og Daglig Leder Digital Truth ltd

VEDLEGG B UTFYLLENDE KOMMENTARER OM ELEKTRONISKE BEVIS

Innledning

"Digital Forensic Science Research Workshop" (DFRWS) har definert "digital forensics" som:

"Bruk av vitenskapelig utviklede og beviste metoder for å ta vare på, samle, validere, identifisere, analysere, tolke, dokumentere og presentere digitale bevis hentet fra digitale kilder i den hensikt å bidra til rekonstruksjon av hendelser som er kriminelle, eller for å hjelpe til med å forutse uautoriserte hendelser som kan være forstyrrende for normale operasjoner."[4]

Når man samler elektroniske bevis, må man benytte en vitenskapelig akseptert metode, akkurat som når man samlet inn DNA prøver, tar fingeravtrykk, måler promille eller fart. Jeg skal eksemplifisere litt:

En erfaren politimann vil kunne skjønnsmessig vurdere om en bil kjører over eller under fartsgrensen. Videre kan det argumenteres at det er mer effektivt at en politimann tar en fartskontroll alene enn at man har to personer involvert i operasjonen.

Ut fra tiltro til politimannens integritet og evner og i tillegg med vurdering av økonomiske kriteria, kan man så argumentere at fartskontroller kan utføres uten nødvendig måleutstyr, og basert på skjønn, uten mulighet til reell overprøving. Retten vil nesten alltid tillegge politimannens utsagn størst troverdighet, og den angivelige lovovertrederen blir sittende igjen med byrden med å bevise uskyld.

De færreste vil godta en slik praksis. Likevel er dette en praksis som tilsynelatende godtas uten motforestillinger når det gjelder digitale bevis.

Beviskjede (chain of custody)

Jeg viser igjen til (ISC)2 CISSP Common Body of Knowledge (CBK) hvor det står:

"*Kjernen i effektiv håndtering av bevis og i særdeleshet elektroniske bevis, er å vise en ubrutt beviskjede for å sikre ekthet og korrekthet av materialet.*

Beviskjeden refererer seg til hvordan bevis håndteres, og det må etableres en beviskjede for hele bevisets livssyklus, fra beviset identifiseres til det destrueres eller returneres til eieren eller arkiveres. Skikkelig bevishåndtering krever at man følger formelle, veldokumenterte prosesser. ***Ethvert brudd i beviskjeden kan så tvil om integriteten av beviset og om profesjonaliteten til de personer som er involvert i etterforskningen av eller innsamling av bevis.*** *Dokumentasjon skal redegjøre for:*

1. *Hvem*
2. *Hva*
3. *Når*

[4] Lærebokteksten som det refereres til i dette kapittelet er en oversettelse av deler av emneområdet "Legal, Regulations, Investigations and Compliance" teksten fra det internasjonalt anerkjente CISSP CBK pensumet. Den originale teksten er på engelsk.

4. *Hvor*
5. *Hvordan*

Dette skal være en integrert del av en standard operasjonsprosedyre som skal brukes i alle saker."

Videre i pensumet heter det:

"Digital Computer Forensics er ikke hardware eller software, men en samling av prosedyrer og rutiner som er:

1. *Metodiske*
2. *Gjenskapbare*
3. *Forsvarbare*
4. *Etterprøvbare"*

Lekkasjesaken

I denne saken har vi "politimannen som på øyemål vurderer en fartsovertredelse, stopper bilisten og utsteder en bot". Politimannen blir så trodd av retten. Tilbake står "en bilist" som må bevise uskyld. Hadde anerkjente regler for digital bevisinnsamling blitt fulgt, ville man kunnet ettergå alle ledd i prosessen med å samle og analysere digitale bevis. Dersom prosessen hadde blitt godt dokumentert og faglig forsvarlig gjennomført, ville jeg som uavhengig gransker ikke ha funnet noe å sette fingeren på.

Vi vet *hvem* som satt opp fellen, dette er grundig dokumentert gjennom politiets forklaring. Vi vet lite om "hva", ingenting om "når" og en del om "hvor" og "hvordan". Men alt vi vet stammer fra en enkelt kilde, uten noen form for støttende dokumentasjon.

Vi vet ikke om det kan ha vært andre inne i prosessen, tilsiktet eller utilsiktet, men vi har erklæringer gitt i bakkant om dette. Det foreligger ikke noe loggingsmateriale som kan støtte disse forklaringene.

Logging

Jeg forventer som et minimum logging som eksemplifisert i følgende tabell:

Dato/tid	Operasjon	Resultat	Merknader
05.01.2012 13:50	Hentet bildemateriale fra hovedbeslag	Vellykket	Hentet fra filserver, område: 98535
05.01.2012 14:25	Valgt ut 3 bilder for å endre detaljer	Valgt 010102.JPG, 010385.JPG, 001346.jpg	Lagt over på isolert maskin, ID 35557, laptop som holdes innelåst, redigert med Photoshop CS versjon 5.2.1

06.01-2012 08:00	Startet arbeid med å legge inn Digimarc. Liste over hvilke advokater som får hvilket Digimarc generert	Liste Digimagic.txt laget	Laget unike Digimarc for alle advokater
06.01-2012 14:35	Politibetjent Hansen starter arbeidet med å kvalitetskontrollere innlagte Digimarc.	Ett avvik oppdaget og korrigert	Avvik på Pettersens CD
06.01-2012 18:35	Politibetjent Hansen avslutter kvalitetskontroll og signerer for at alle utleveringer har korrekt Digimarc	Signert bevislogg	Materiale innlåst i safe etter gjennomgangen.

Som det fremgår av eksemplene, er ikke dette noe som krever noe stort eller særlig arbeidskrevende opplegg, kun at data fanges (og sikres for etterprøvbarhet) etter hvert som de oppstår. Slik fangst kan skje i form av notater i en journal, en tekstfil på et datasystem eller ved å diktere meldinger inn på en diktafon.

Hensikten er å gi etterprøvbarhet. Dersom en gransker for eksempel ser at det ble generert unike Digimarc for alle 170+ bistandsadvokatene, men at dette skjedde på 3 minutter, vil det være meget relevant å stille spørsmål omkring prosessen, verktøy benyttet etc.

Prinsippene for håndtering av digitale bevis skal være velkjente for politiet. Når de i denne sammenhengen velger å fravike alle fornuftige, relevante og faglig aksepterte rutiner, ser jeg kun tre mulige motiver for dette:

1. Tidsnød
2. Mangel på kompetanse
3. Ønske om ikke å bli etterprøvd

Relevante krav om dokumentasjon av politiets handlinger er ignorert. Dette setter rettsikkerheten i fare og åpner for at feil kan forbli uoppdaget.

AVSLUTTENDE MERKNADER

Det er dessverre ikke uvanlig at elektroniske bevis aksepteres av norsk rettsvesen uten den nødvendige kvalitetsvurdering. Politiets eksperter uttaler seg, og mot dem er det vanskelig å argumentere, spesielt når man ikke gis innsyn i alt bevismateriale eller når bevismateriale helt mangler. Dessuten vil de færreste ha ressurser til å leie inn en egen datateknisk gransker.

Resultatet av den fraværende dokumentasjonen gjør at vi har et "politimann på fartskontroll uten fartsmåler" scenearie i denne saken. Politimannens skjønn og vurderinger legges til grunn for domsavsigelse. Den anklagede må bevise uskyld.

Den ukritiske aksepten av elektroniske bevis, uten at veletablerte (og for politiet velkjente) internasjonale rutiner for kvalitetssikring benyttes, setter rettsikkerheten i alvorlig fare.

Basert på fremlagt og innhentet materiale (herunder politiets egne dokumenter og redegjørelser til Oslo Tingrett mottatt fra advokat Sjødin), min fagkunnskap, erfaring og beste skjønn, etter å ha gjort min vurdering av de fremlagte elektroniske "bevis" med støttende forklaringer, fravær av nøkkelopplysninger i saken, beviste prosedyrefeil og den særdeles dårlige etterretteligheten i de elektroniske "bevisene", er det ikke mulig å bevise at lekkasjen kommer fra Klomsæts kontor.

Legger man til grunn vitneutsagn og skriftlig erklæring fra ansatte i advokatfirmaet Klomsæt & co as som tilstedeværende personer (samt advokat Mehus) på Klomsæts kontor den 3. februar 2012, tidsaspektet, Sigurd Klomsæts fysiske fravær fra kontoret, de påviste svakhetene i Digimarc systemet, svakhetene i valgt krypteringsløsning, politiets prosedyrefeil, pressens tilgang til omfattende bildemateriell før Klomsæt får dette i sin besittelse, bildet av Brevik i politiuniform som dukket opp på nettet i desember 2011 samt tidligere lekkasjer av materiell som bistandsadvokatene ikke har hatt tilgang til, så fremstår det som meget usannsynlig at denne lekkasjen kommer fra Klomsæts kontor.

Oslo 02/11-2012

Stein A. J. Møllerhaug
CISSP, Certified CISSP Trainer,
Certified ISO 27001 Lead Auditor Trainer
Rådgiver og Daglig Leder Digital Truth ltd

VEDLEGG C, TIDSLINJEDATA

Vedlegget viser tidslinjen for behandling av den aktuelle CDen. Som det fremgår av tidslinjen har arbeidet pågått siden 6/12-2011. På grunn av politiets manglende dokumentasjon har jeg kun tidspunktet for opprettelse av en fil og siste endring av filen. Jeg kan ikke vite hva som har skjedd med filen mellom disse to tidspunktene.

Siste endring på Sigurd Klomsæts CD skjer mandag 30/1 2012 klokken 20:19:33. Pressen viser det første bildet fredag 3/2-2012. Det går således nesten 4 døgn fra CDen er ferdig laget til pressen viser bildene.

Materialet er i denne perioden i politiets forvaring. Det er kun de siste timene at politiet ikke har eksklusiv kontroll med materialet. Rent statistisk sett er sjansen for en lekkasje av det ferdige materialet overveldende mye større mens det er i politiets besittelse enn mens det er tilgjengelig for ansatte ved Sigurd Klomsæts kontor.

Lekkasjen kan dessuten ha inntruffet når som helst fra det tidspunktet politioverbetjent Hafredal bestemmer seg for hvilke "Image ID" som skal benyttes, da lekkasje av bildet og "Image ID" kan ha skjedd som to uavhengige operasjoner.

Oslo 02/11-2012

Stein A. J. Møllerhaug
CISSP, Certified CISSP Trainer,
Certified ISO 27001 Lead Auditor Trainer
Rådgiver og Daglig Leder Digital Truth ltd