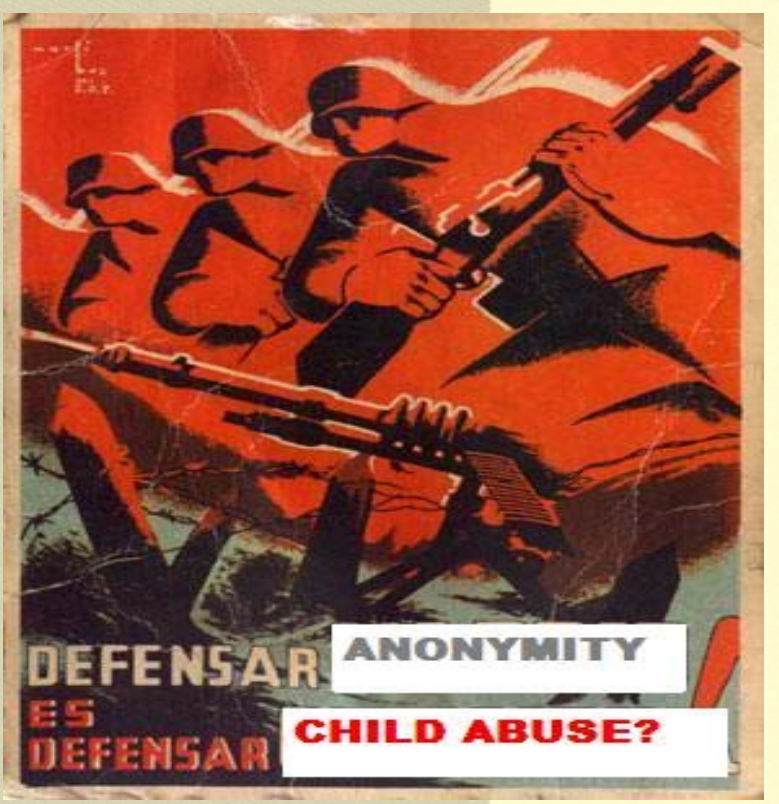
Høgskolen i Nesnas skriftserie

Nr. 63 Høgskolen i Nesna 2005

INTERNETT som verktøy for formidling av overgrepsbilder

Studentrapporter fra 1. år IT-Bachelor



Per A. Godejord (Red.)

Pris: Kr. 152
ISBN: 82-7569-119-2
ISSN: 0805 - 3154

HØGSKOLEN I NESNA

Abstract

This pamphlet consists of five student reports.

Three of the reports give a thorough description and analysis of the system called Freenet. Freenet is free software which lets you publish and obtain information on the Internet without fear of censorship. To achieve this freedom, the network is entirely decentralized and publishers and consumers of information are anonymous. Without anonymity there can never be true freedom of speech, and without decentralization the network will be vulnerable to attack.

Communications by Freenet nodes are encrypted and are "routed-through" other nodes to make it extremely difficult to determine who is requesting the information and what its content is.

Users contribute to the network by giving bandwidth and a portion of their hard drive (called the "data store") for storing files. Unlike other peer-to-peer file sharing networks, Freenet does not let the user control what is stored in the data store. Instead, files are kept or deleted depending on how popular they are, with the least popular being discarded to make way for newer or more popular content. Files in the data store are encrypted to reduce the likelihood of prosecution by persons wishing to censor Freenet content.

The students who did the assignment on Freenet discuss some possibilities on how to investigate this system, as opposed to the more standard P2P networks. One student group also asks a fundamental question – If child pornography in the cache of a computer is considered not to constitute possession, what then if the data storage on your Personal Computer used by Freenet is filled with child pornography?

The last two groups have looked at anonymous proxies and the possible use of this tool in illegal activities.

Anonymous proxies may be described as a cloak that sits between your computer and any web sites you visit. It prevents the web sites you visit from finding out who you are. And it can use the standard SSL protocol to encrypt all communication from your browser, so that no one (except for provider of the anonymous proxy) knows where you are surfing. Without the proxy, you are connected directly to the machines you visit.

Using an anonymous proxy you might download child pornography without leaving a trace, but are you really anonymous? And do anonymous proxies constitute a threat to the system of “child porn filter”, designed by the Norwegian National Criminal Investigation Service and Telenor?

Innhold

DEL 2 ANONYME PROXYER

Gå inn i din tid!

Kringsatt av fiender,
Gå inn i din tid!
Under en blodig storm –
Vi deg til strid!

Disse linjene fra Nordal Griegs dikt ”Til ungdommen” fra 1936 danner en innholdsmessig ramme rundt undervisningsprosjektet ”Gå inn i din tid!”. Og med et tema så alvorlig som overgrep mot barn, og distribusjon av billedmateriale av slike overgrep på Internett, så passer det også å sitere noen linjer av Arnulf Øverland:

Du må ikke sitte trygt i ditt hjem
Og si: Det er så sørgelig, stakkars dem!
Du må ikke tåle så inderlig vel
Den urett som ikke rammer deg selv!
Jeg roper med siste pust av min stemme
Du har ikke lov å gå der og glemme!

”Det er så sørgelig, stakkars dem!” er vel kanskje det vi aller helst vil nøye oss med. En kjapp ettertanke etter å ha lest en eller annen overfladisk artikkel i Dagbladet og så videre til andre og nærere ting. For dette er jo ikke noe som angår oss. Eller er det kanskje det?

”Gå inn i din tid!” er et undervisningsprosjekt ved vårt Bachelorstudie i Informatikk, som bunner i en overbevisning om at IT-studenter må læres opp til å ha et fokus ikke bare på det tekniske, men også på det menneskelige. Prosjektet er en del av kurset Samfunnsinformatikk (IN116), og vårt håp er at dette prosjektet skal gi studentene en praktisk innfallsvinkel til de tema som omfattes av Samfunnsinformatikk.

Via dette prosjektet får de innføring i både jus, etikk og samfunnsrelatert informasjonsteknologi, samt en anledning til å utføre samfunnsnyttig tjeneste i samarbeid med Redd Barna og NyeKRIPOS.

For å sitere en uttalelse den New York baserte juristen, forfatteren og forkjemperen for barns rettigheter, Andrew Vachss kom med i forbindelse med HiNes prosjekt: ”—it offers them a chance to serve on the front lines of the only war *always* worth fighting.”

I dette heftet er vi stolte over å kunne presentere fem rapporter som er utført av våre førsteårsstudenter i Samfunnsinformatikk, over tema som har sitt utgangspunkt i en ide fra NyeKRIPOS.

Rapportene omhandler to tema – Freenet og anonyme proxyer.

FreeNet er et peer-to-peer nettverk. I motsetning til server/klient nettverk hvor all informasjon ligger sentralt på en maskin og alle brukere kobler seg opp mot denne maskinen for å laste ned filer, ligger de forskjellige filene i et P2P-nettverk på private datamaskiner verden over og man bruker programvare for å finne de filene man vil for så å laste dem ned. Et godt eksempel på et peer-to-peer nettverk er Gnutella, hvor den mest kjente klient programvaren er Kazaa. Et annet eksempel som de fleste sikkert har hørt om er Napster, som satte musikkbransjen i kok.
FreeNet skiller seg fra de vanlige P2P-nettverken på flere måter.

FreeNet kan best beskrives som en adaptiv peer-to-peer nettverksapplikasjon som tillater publisering, replikering og henting av data mens anonymiteten til både forfattere og lesere blir ivaretatt. FreeNet opererer som et nettverk av identiske noder som kollektivt samler sin lagringskapasitet til å lagre datafiler og samarbeider med å route spørringer etter data til den mest sannsynlige fysiske beliggenheten på nettet. Filer er referert til på en lokasjons uavhengig måte, og blir dynamisk replikert på maskiner nært den som spør etter filen og slettet fra maskiner hvor filen ikke blir etterspurt. Det er usannsynlig (umulig) å finne utgangspunktet for en gitt fil som passerer gjennom nettverket og vanskelig for en node eier å kjenne til eller bli holdt ansvarlig for det fysiske innholdet i den delte katalogen (datastoren) på sin egen maskin (node).

Alt i Freenet er kryptert, også det som lagres på din PC når du er en del av Freenet. Juridisk er det svært interessant, med tanke på tidligere rettsavgjørelser i forbindelse med overgrepsbilder i datamaskinens ”cache”. Hvis man ikke kan dømmes for besittelse av overgrepsbilder man måtte ha liggende i nettleserens mellomlager, hva da med overgrepsmateriale som er kryptert og ligger på en lagerplass tilordnet Freenet, og som man kan påstå man ikke hadde anelse om med henvisning til Freenet sitt system med mellomlagring av filer på alle noder i nettet?

En Proxy er et program på en PC/server som er tilknyttet en spesiell port på PC-en hvor den er installert, og som i utgangspunktet var ment for å utføre sikkerhetstjenester samt andre funksjoner som web- og innholdscaching. Et godt ord for en Proxy er mellomledd.

Dersom du befinner deg bak en proxy-server vil ikke din maskinens ip-adresse være synlig for andre bruker på Internett. De vil kun se ip-adressen til proxy-serveren. En proxy-server kan benyttes i to situasjoner: internt i et lokalt nettverk eller som webproxy på Internett.

Er proxyen satt opp internt i et nettverk vil ikke klientene i nettverket være synlig for omverdenen. Dette betyr at man surfer anonymt på Internett, og en hacker vil ikke kunne identifisere ip-adressen, nettleser, operativsystem eller annen informasjon til en bedrifts pc-er.

Måten dette gjøres på er at proxyen bytter ut ip-adressen til klienten med sin egen IP før forespørselen sendes ut på Internett. Når proxy-serveren får svar tilbake byttes ip-adressene tilbake for så å sendes til klienten.

Er en proxy-server satt opp som en webproxy vil denne kunne brukes av nettlesere og andre programmer som bruker Internett som kommunikasjonskanal. Scenarioet er det samme som over. Du sender en forespørsel ut på Internett der målet er proxy-serveren. Proxy-serveren setter sin ip-adresse inn i spørringen, henter ressursen, og sender denne tilbake til klienten. På den måten "lures" både nettsiden du spurte etter, og din ISP. Dersom også nettleverandøren kan la seg lure av at brukerne benytter anonyme proxyer, hva skjer da med det såkalte ”overgrepsbilderfilteret” som NyeKRIPOS og TELENOR har utviklet?

De fem rapportene i dette heftet var utført som obligatoriske oppgaver, og de ble fremført for inviterte gjester fra media og politi den 6. april 2005.

Alle rapportene er analyseoppgaver og utført i henhold til HiNes retningslinjer og Norsk lov.

Mo i Rana, 1. mai 2005

Per Arne Godejord
Førstelektor
Seksjon for informatikk
Høgskolen i Nesna

Freenet

Ytringsfrihet til hvilken pris?

Jarle Hagavei

Jørn Ivar Remmen

Hans Petter Hammer

Bachelor Informatikk
Høgskolen i Nesna avd. Mo i Rana
Mars 2005

Innledning

Filosofien bak Freenet

Frihet er et vidt begrep og inneholder mange fasetter som vi i den vestlige verden tar for gitt, men som mange i andre deler av verden bare kan drømme om, de kan ikke engang snakke om slike ting fordi det kan få fatal konsekvenser for dem og deres familier. Og da mister man med en gang en vital del av det som faktisk gjør oss til det vi er; mennesker. Det å kommunisere tanker og ideer er det som skiller oss fra resten av dyreverdenen og derfor definerer oss som art. Kommunikasjon er det som har ført oss inn i det tjueførste århundre og som sannsynligvis skal ta oss videre inn i neste årtusen.

De fleste mennesker som blir spurt om de vil vite noe eller ikke, velger som regel det første. De fleste mennesker har en trang til å samle informasjon om verden rundt seg, om ikke for å bidra til å gjøre verden bedre, så i alle fall av ren nysgjerrighet. Det er en iboende egenskap hos mennesker å ønske å vite, i det hensende er vi alle oppdagelsesreisende. Selv i de landene hvor det rett og slett er farlig å snakke om alt som måtte passe en å snakke om, og ikke minst vite alt som en ønsker å vite, er fortsatt ønsket om å vite og å snakke meget stort. Mennesker har gjennom historien vært villige til å dø for å få sagt sitt eller få hørt hva de andre hadde å si. Ideer og tanker har bestandig blitt utvekslet blant mennesker i alle år, og er en av de viktigste byggesteiner til vår sivilisasjon.

I det gamle Hellas ble det 400 år før Kristus innført en ny styreform som ble kalt demokrati. Ordet demokrati er sammensatt av de to greske ordene Demos og Kratien, som betyr henholdsvis Folket og Styre. Demokrati er i essens ideen om at retten til å fatte beslutninger på vegne av fellesskapet utgår fra folket selv. Ideen om politisk likhet, det vil si at alle skal ha den samme retten til å delta i samfunnsstyringen. 140 av verdens nærmere 200 land holder i dag flerpartivalg, 106 av disse begrenserer sivile og politiske rettigheter.

Noen regjeringer i verden, f.eks. Kina, sensurer alt fra omverden som de finner upassende for befolkningen, altså alt som kan være med på å opplyse folket og eventuelt svekke styresettets posisjon. Ytringsfriheten er viktig for at et demokrati skal virke ut fra de grunnleggende prinsipper. Den eneste måten å sikre at demokratiet vill forbli reelt og effektivt er å forsikre seg mot at regjeringen ikke kan kontrollere befolkningens evne til å dele informasjon og til å kommunisere. Så lenge alt vi ser og hører er filtrert og sensurert, er vi ikke fri i ordets sanne betydning.

Men man kan ikke ha ytringsfrihet uten mulighet for anonymitet. Det meste av sensur er retrospektivt, fordi det generelt sett er mye lettere å komme de som snakker til livs etter at de har sagt noe enn det er å forhindre dem i å si noe. Den eneste måten å forhindre represalier fra myndighetene for noe man har sagt er å forbli anonym. Det er en vanlig missoppfatning at man ikke kan stole på anonym informasjon. Det er ikke nødvendigvis slik at informasjon fra en anonym kilde ikke kan tas på alvor. Hvis man bruker en digital signatur kan man lage seg et anonymt pseudonym, som folk med tiden kan lære seg å

stole på. Ytringsfrihet er en vital del av demokratiet og er noe som vi tar som en selvfølge. Ytringsfrihet er den mekanismen som gir folket muligheten til å kontrollere sine respektive regjeringer gjennom utveksling av korrekt og usensurert informasjon. Uten fullstendig ytringsfrihet ville det blitt umulig å treffe de riktige valg når det kommer til å velge de representantene som skal styre landet og dermed ta avgjørelser som får konsekvenser for alle innbyggerne i landet. Tenk deg nå at noen hadde muligheten til å kontrollere den informasjonen du hadde tilgang til. Dette ville gi dem muligheten til å manipulere dine meninger ved å tilbakeholde eller endre fakta, lyve og sensurere informasjon som motsir disse løgnene. Dette er ingen fantasi skapt av Orson Wells, det er faktisk standard praksis for vestlige myndigheter å lyve for befolkningen, faktisk så vanlig at folk regner med det, selv om dette underminerer de demokratiske prinsipper som rettferdiggjør regjeringen i utgangspunktet.

Det er ikke like selvfølgelig for alle mennesker på denne lille planeten vår at man kan si og mene hva man vil uten at dette får konsekvenser, og derfor er det viktig at de som skal si noe har muligheten til å gjøre det og fortsatt forbli anonym. Disse synspunktene er kjernen i filosofien bak en avhandling skrevet av Ian Clarke mens han studerte IT ved universitetet i Edinburgh i Skottland. Avhandlingen het; " A Distributed Decentralised Information Storage and Retrieval System"[1]. Freenet er et direkte resultat av denne avhandlingen. Ian Clarke startet Freenet prosjektet i 1999 og er fortsatt prosjektets koordinator.

Generelt om Freenet

Freenet er et peer-to-peer nettverk. I motsetning til server/klient nettverk hvor all informasjon ligger sentralt på en maskin og alle brukere kobler seg opp mot denne maskinen for å laste ned filer, ligger de forskjellige filene i et P2P-nettverk på private datamaskiner verden over og man bruker programvare for å finne de filene man vil for så å laste dem ned. Et godt eksempel på et peer-to-peer nettverk er Gnutella, hvor den mest kjente klient programvaren er Kazaa. Et annet eksempel som de fleste sikkert har hørt om er Napster, som satte musikkbransjen i kok.
Freenet skiller seg fra de vanlige P2P-nettverken på flere måter.

Freenet kan best beskrives som en adaptiv peer-to-peer nettverksapplikasjon som tillater publisering, replikering og henting av data mens anonymiteten til både forfattere og lesere blir ivaretatt. Freenet opererer som et nettverk av identiske noder som kollektivt samler sin lagringskapasitet til å lagre datafiler og samarbeider med å route spørringer etter data til den mest sannsynlige fysiske beliggenheten på nettet. Filer er referert til på en lokasjons uavhengig måte, og blir dynamisk replikert på maskiner nært den som spør etter filen og slettet fra maskiner hvor filen ikke blir etterspurt. Det er usannsynlig (umulig) å finne utgangspunktet for en gitt fil som passerer gjennom nettverket og vanskelig for en node eier å kjenne til eller bli holdt ansvarlig for det fysiske innholdet i den delte katalogen (datastoren) på sin egen maskin (node).[2]

[1] http://Freenetproject.org/Freenet.pdf

[2] http://Freenetproject.org/Freenet.pdf

Freenet er software som du laster ned og installerer på din maskin. Når du gjør dette oppretter du en “node” på din maskin. Denne noden har tre hovedkomponenter; et web basert brukergrensesnitt, en katalog som deles på nettverket på lik linje med andre peer-to-peer nettverk og en Proxy server som sørger for en del av anonymiteten i Freenet. Når du publiserer en fil på Freenet så krypteres den i det øyeblikket du publiserer og du blir sittende igjen med en kryptert adressestreng (en nøkkel) som kan brukes til å hente filen fra hvor den måtte befinne seg på Freenet. Og dette er verdt å kommentere videre. Når en fil publiseres så publiseres den ikke til en bestemt lokasjon på Freenet, den publiseres til flere tilfeldig valgte maskiner, slik at du ikke vet hvor kopiene av den befinner seg. Dette gjør det umulig å slette denne filen etter at den er publisert. Eierne av de maskinene, heretter kalt nodene som filen blir publisert til vet ikke at de har mottatt denne filen og kan heller ikke gjøre noe med den. Dette fordi alt som blir lagret i den delte katalogen er kryptert. Når du har lastet opp en fil til Freenet så skal den befinne seg i nettverket til all ettertid. Dette er i alle fall meningen, men filer forsvinner allikevel ut av Freenet på grunn av en egenskap ved Freenet, nemlig størrelsen på den delte katalogen og måten filer blir spredt gjennom nettverket. En fil som blir mye etterspurt og hyppig lastet ned sprer seg gjennom Freenet og blir lagret på all noder mellom kildenoden og den noden som spør etter filen. Mens filer som ikke blir etterspurt blir til syvende og sist blir skjøvet ut av Freenet på grunn av størrelsen til den delte katalogen på de forkjellige nodene. Dette er opplagt og enkelt å forstå. Den delte katalogen har en fast størrelse som du selv kan bestemme og kan dermed bare romme et vist antall filer. Når denne katalogen er full og det kommer nye filer inn gjennom nettverket så blir gamle filer overskrevet, og dermed vil filer som ikke blir etterspurt og dermed spredt, forsvinne ut av nettverket sakte men sikkert.

Publisering på Freenet kan skje på flere måter og man kan publisere hva det måtte være, lovlig eller ei. Den enkleste måten å publisere en fil inn i Freenet på er å bruke det web baserte brukergrensesnittet og laste opp filen derfra. Når man gjør dette blir filen man velger spredt ut på nettet og man blir sittende igjen med en nøkkel som identifiserer denne filen. Med denne nøkkelen kan man laste ned filen igjen, eller man kan distribuere denne nøkkelen slik at andre som før denne nøkkelen kan laste ned filen. Det blir generert flere typer nøkler, disse blir forklart i detalj senere i rapporten. En annen måte å publisere materiale inn i Freenet på er å lage en webside kodet i HTML (Hyper Text Markup Language), språket som de aller fleste statiske internettsider er skrevet i, og så laste denne opp i Freenet. Disse sidene kan du gi et hvilket som helst innhold og også her blir du sittende igjen med en kryptert nøkkel som i dette tilfellet blir adressen til siden. Innholdet på denne siden blir også kryptert og hver del av innholdet får en egen nøkkel som brukes til nedlastning av materialet.

I tidligere utgaver av Freenet så kunne man ikke publisere fra det webbaserte brukergrensesnittet, og man kunne heller ikke søke etter filer. Man kan fortsatt ikke søke etter filer og data ved navn, men man kan nå søke etter spesifikke nøkler nå, og man kan altså publisere fra samme sted.

Dette webbaserte brukergrensesnittet, som vi så pent og teknisk kaller det er ikke mer enn en meget sparsom “internettside” som du ser på gjennom din nettleser, som f.eks. MS Internet Explorer, Mozilla eller Opera.
Man kan jo stille seg spørsmålet; “men hvordan skal resten av brukerne på Freenet få tak i de filene man laster opp når alt er kryptert og må hentes tilbake med nøkler som bare den som publiserer blir sittende med?” Og svaret er at man må på en eller annen måte få spredt disse nøklene slik at de som vil kan få lastet ned filene du har publisert. Det er selvfølgelig mange møter å gjøre dette på. Du kan ta med deg den nye nøkkelen og komme på besøk til meg, du kan sende den i posten eller stille deg på torget og rope den ut.
En annen måte er å få publisert disse nøklene som lenker via såkalte Freenet portaler, noe vi liker å kalle indekssider. Disse sidene inneholder publiserte nøkler som fører til publiserte sider på Freenet men alskens innhold. En annen og kanskje mer brukt metode i de kretser hvor innholdet bak nøkkene er dokumenterte seksuelle overgrep mot barn, er den krypterte Freenet utgaven av IRC (Internet Relay Chat), et chatteverktøy hvor du kan opprette egne private kanaler, egne private chatterom. Her møtes likesinnede for å utveksle siste nytt i form av nøkler til innhold de har publisert. Uansett hvilken metode en benytter seg av, så er fortsatt poenget å få distribuert disse nøklene slik at de andre på Freenet kan få tilgang til det du har publisert. Og det er nok ikke vanskelig å forstå at hvis det gjelder distribusjon av nøkler som leder til ulovlig materiale så vil nok også distribusjon av disse nøklene være en lyssky aktivitet.

Det kan her tas med at når du installerer Freenet og åpner det webbaserte brukergrensesnittet så blir du presentert for fem “lenker” til slike portaler som vi snakket om i sted, hvor flere hundre slike Freenet sider er lagt ut “offentlig”. En av disse portalene heter “The Freedom Engine” og inneholder flere hundre lenker til sider med innhold fra tanker om verden til terrorisme. Og selvfølgelig inneholder denne portalen flere lenker til sider som reklamerer for å inneholde dokumenterte seksuelle overgrep mot barn. Publisering av nøkler til disse portalene skjer anonymt slik at ingen kan bli tatt for å publisere slikt materiale og man trenger heller ikke skjule det eller pakke det inn i noe annet. Det ligger åpent i dagen og alle som går inn på disse portalene som “The Freedom Engine” får tilgang til slikt materiale ved et enkelt tastetrykk. Når man publiserer til en slik side blir den nøkkelen man publiserer siden under offentliggjort gjennom den lenken som blir opprettet i portalen. Det betyr at så snart en side er publisert til en portal, er det bare for alle som besøker portalen og klikke seg inn på den siden via lenken som bare er en HTML forkledd nøkkel. Slik vi kjenner det fra Internet; at navnet på lenken trenger ikke engang ligne på adressen som lenken peker til. For eksempel kan det på en internettside så ”Nyheter” som er en lenke med adressen www.vg.no. Slik er det da altså når en ”freesite”, en side på Freenet publiseres til en slik portal. Man trenger bare å klikke på de lenkene man ser og kommer direkte til den siden som lenken (nøkkelen) peker til. Og siden disse sidene som inneholder dette materialet er spredt gjennom Freenet som en hvilken som helst annen publisert fil, og i tillegg er kryptert i de delte katalogene på de nodene det befinner seg på, så er det umulig å slette dette materialet fra Freenet.

Den eneste måten at dette materialet forsvinner fra Freenet er på den måten vi snakket om tidligere, nemlig at filene ikke blir etterspurt, og dermed blir skjøvet ut til fordel for filer

som blir etterspurt. Ironisk nok er det en målsetting for skaperne av Freenet at all data publisert på Freenet etter hvert skal bli lagret til evig tid. Det oppfordres til å opprette permanente noder med større og større lagringskapasitet slik at filer ikke blir skjøvet ut. En permanent node er ikke annet enn en maskin som alltid er koblet til Internet og som hele tiden kjører Freenet. I motsetning til en ikke permanent node som for eksempel kan være en maskin med modem oppkobling, hvor maskinen ofte er av nettet.

Denne oppfordringen om å opprette permanente noder er i tråd med filosofien bak Freenet og går selvfølgelig på dette med ytringsfrihet og er ment å sikre at den informasjonen som folk vil dele med resten av verden ikke skal forsvinne før flere har fått lest, sett eller hørt hva forfatteren har å si. Med tanke på land hvor politiske ytringer ikke bestandig blir belønnet med ros og heder, men i stedet med en kule betalt av familien, så er det forståelig at en vil bevare den informasjonen som strømmer inn i Freenet, men slik tilstanden til Freenet er i dag, kan man stille seg spørsmål ved om det er verdt det, og om Freenet er blitt hva skaperne ønsket eller ikke. Mye av innholdet i Freenet i dag er av grafisk karakter, og mye av dette er av ulovlig natur. Vi kommer tilbake til innhold på Freenet senere i rapporten.

Når du har fått en nøkkel som peker til en spesiell fil, eller side på Freenet og bruker denne til å se på eller laste ned innholdet skjer en rekke ting. Når du bruker en slik nøkkel sender du en spørring ut på Freenet til nærliggende noder om noen har denne filen som nøkkelen peker til. For å unngå at disse spørringene bare går rundt og rundt i Freenet til evig tid, og dermed danner uendelige løkker blir hver spørring begrenset med noe som heter “Hops To Live”, forkortet HTL. Dette er en begrensning lagt inn i spørringen på hvor mange noder spørringen skal gå over. Hvis HTL blir satt til 25 vil spørringen gå ut til 25 noder før den dør. HTL blir redusert med en' for hver node den spør. Hvis spørringen ikke finner filen som hører til nøkkelen som blir brukt på den første noden så spør den neste node og fortsetter slik til den finner filen eller HTL utløper. Hvis spørringen ikke finner den filen nøkkelen peker til så returneres en beskjed om at filen ikke kunne finnes, og spørringen må eventuelt sendes ut på nytt. Freenet tar seg av dette automatisk og fortsetter å spørre nye grupper med noder til den finner filen eller til brukeren avbryter spørringen. Hvis filen blir funnet så returneres denne til den som har spurt etter den, og filen kan da ses på, høres på, leses, eller lagres til harddisken på maskinen. Når en spørring med en nøkkel finner filen som hører til nøkkelen og returnerer denne til den noden som satte ut spørringen blir som sagt filen sendt tilbake til den som spurte etter filen, men den blir ikke sendt direkte fra den noden den befinner seg på til den noden som spurte etter filen. Filen blir sendt nedover nodene i mellom den noden hvor filen befinner seg og den noden som spurte etter filen. Og alle filer som sendes slik lagres på alle noder i mellom sender og mottaker. Dette betyr at hvis du spør etter en fil, bruker en nøkkel til å laste ned et bilde, eller bruker en av lenkene til en av portalene for å se en side, så er du med på å spre materialet du ber om på Freenet. Dette har selvfølgelig uheldige konsekvenser når det er snakk om ulovlig materiale, være det seg sider om drap, terrorisme eller overgreps bilder av barn. Freenet er meget tregt til å begynne med når man setter opp en node, men blir raskere etter hvert som materiale blir spredt og din node lærer seg sine nabonoder å kjenne og dermed får en oversikt over hvilke noder spørringer skal sendes til i fremtiden.

Enhver node i Freenet har i tillegg til den delte katalogen en routingtabell med en oversikt over de nærliggende noder og deres nøkler. Denne tabellen ligger i den delte katalogen og er også kryptert slik at en kan ikke hente informasjon om nodene som er listet der.

Hoveddel

Dokumenterte seksuelle overgrep mot barn på Freenet

Dokumenterte seksuelle overgrep av barn, heretter referert til som overgrepsbilder har eksistert i årevis i en eller annen form og spredning av denne type materiale har fulgt enhver teknologi som har dukket opp. Som en av KRIPOS etterforskere poengterte var oppfinnelsen av polaroid kameraene et stort fremskritt for de som produserer og distribuerer overgrepsbilder, siden de slapp å løpe risikoen ved å levere filmen inn for fremkalling.

Da Internet ble født fikk disse overgrepsbildene ny føtter å gå på og vi opplevde en eksplosjon av overgrepsbilder og videoer. Dette førte til at etterspørselen av slikt materiale ble større, og dermed økte produksjonen også. Barn verden over blir utsatt for grovere og grovere overgrep for å mette en syk etterspørsel, og Internet har vært den ideelle markedsplass for distribusjon av slikt materiale. Når peer-to-peer nettverkene som Bearshare, Gnutella og Napster kom til verden kunne privatpersoner dele sine filer ved å dele en katalog på sin maskin og ved hjelp av programvare som Kazaa, Limewire og Shareaza kunne de søke etter og laste ned det de andre hadde delt. Dette førte til enda større utbredelse av ulovlig materiale, men er også skummelt for de som driver med det på grunn av at det ikke finnes noen som helst anonymitet innbakt i disse systemene. I Shareaza for eksempel kan du søke på filnavn og får opp en mengde treff på søket. Og i søkeresultatet ser du hvilke maskiner som huser filen du søkte etter, med full IP adresse og muligheten til å se alle filene som den maskinen inneholder. Dette er utrygt for de som driver med ulovligheter.

Og her kommer Freenet inn i bildet og viser seg som det mest perfekte mediet for distribusjon av overgrepsbilder. På grunn av filosofien bak Freenet og dermed måten Freenet er oppbygd på kan man distribuere en hvilken som helst fil med total anonymitet. Dette gjør at Freenet er den ideelle samlingsplass for personer som driver med lysskye aktiviteter, som blant annet overgrepsbilder. Og dessverre frykter vi at det kan være mye av vederstyggeligheten der ute på Freenet. Denne frykten er basert på våre observasjoner av noen av disse portalene. Det ligger åpent i dagen på disse portalene lenker direkte til sider med overgrepsbilder. Vi kan for syns skyld ta med at vi kun har sett disse lenkene på portalene og har av åpenbare grunner ikke sett på noe av innholdet bak lenkene. Men når navnene på lenkene er; Hitlers cute kids, Pedophilephile og Kinderfick, så kan man vel tenke seg til hva som befinner seg på disse sidene. Vi kan selvfølgelig i denne sammenhengen nevne at det er en kjent strategi fra markedsføring på Internet å lokke med spennende titler og muligheter for noe ulovlig, for å lokke folk til å klikke på lenken. Slik sett trenger det ikke å være overgrepsbilder bak de lenkene som har disse navnene, men sannsynligheten er overveldende stor. Siden ingenting blir solgt på Freenet er den

eneste sannsynlige formen for juks med slike lenker og nøkler, slik vi ser det, et forsøk fra folk som missliker overgrepsbilder og prøver å gjøre noe med saken.
Problemet her er bare det at hvis disse nøklene er falske vill det snart spres seg rykter om dette, disse nøklene vil bli distribuert som falske og de som driver med ”overgrepsbilder” kan stenge disse nøkkene ute fra sine noder med verktøy som blir beskrevet under ”The Cleanex Project” litt senere i rapporten. Og videre så kan de som er ute etter overgrepsbilder bare unngå disse nøklene, slik at di til syvende og sist blir skjøvet ut av Freenet. Demokrati, ytringsfrihet og anonymitet har sin pris, og dessverre er det mange barn verden over som til daglig betaler denne prisen.

Freenet er så langt vi kan se en av de smarteste løsningene for kriminelle til å få drive med det de måtte ha lyst til uten å kunne bli holdt ansvarlig for sine handlinger. Det at Freenet er med på å bidra til flere seksuelle overgrep av barn og spredning av disse er nok høyst sannsynlig. Siden Freenet er et slik ideelt medium til nettopp det formålet, og med tanke på den sikkerheten Freenet gir til dem som driver med det. Det som kanskje kan være en konsekvens i denne sammenhengen er at Freenet er med på å gjøre disse overgrepene grovere og mer voldelige siden anonymiteten ved Freenet gjør at flere tør benytte seg av slikt materiale og dermed øker etterspørselen. I tillegg tør de som driver med dette gå lengre i sin virksomhet nettopp på grunn av sikkerheten til Freenet. Det tragiske, og ikke minst farlige, er at Freenet ikke har noen som helst form for sensur. Det kan så være at filosofien er grei, og ytringsfrihet ikke bør sensureres for å gi et levedyktig demokrati som alle mennesker er tjent med. Men det er ingen mennesker som er tjent med overgrepsbilder, terrorisme og drap, og det vil nok 95 % av jordens befolkning være enige i.

Freenet kan være et fristed for alle som vil drive med lysskye aktiviteter på nettet uten å kunne bli strafferettslig forfulgt på bakgrunn av sine handlinger. Vi frykter at det er mye overgrepsbilder på Freenet og vi frykter at det bare vil komme mer etter hvert som Freenet vokser. Det er en ond sirkel som er startet hvor Freenet kan bli motoren som bare akselererer sirkelen. Flere og flere overgripere vil kunne oppdage fordelene ved Freenets anonymitet og dette vil kanskje føre til en mer organisert virksomhet når det kommer til overgrepsbilder. Fordi at man fritt kan si og gjøre som man vil på Freenet uten konsekvenser er det ikke vanskelig å forestille seg en utvikling hvor overgripere vil samle seg og dele materiale, avtale møter, arrangere treff og missbruke flere barn. Det finnes en del chatteverktøy på Freenet hvor kommunikasjonen er kryptert og det er vår antagelse at disse blir brukt i både produksjons og distribusjons sammenhenger. Vi må vel kanskje ta med at salg av overgrepsbilder direkte i Freenet ville være veldig vanskelig hvis man skulle opprettholde anonymiteten, for det sier seg selv at hvis du bruker et kreditkort til å betale med for slikt materiale så er du ikke anonym lengre. Så her vil det antakelig mest være snakk om deling av materialet. Vi vet selvfølgelig ingen ting om hvor vidt det blir gjort kjøp og salg via chatterommene, om personer der utveksler betalingsinformasjon og kjøper og selger av hverandre.

Det hadde jo vært til stor fordel for politiet hvis det var tilfelle, for da kunne infiltrasjon av slike chatterom være en strategi for å komme disse personene til livs gjennom den informasjonen de måtte dele om seg selv. Men dette er noe politiet selv får forske videre på.

The Cleanex Project

Heldigvis er ikke alle som bruker Freenet entusiaster av overgrepsbilder, og noen er faktisk så bestemt i mot denne styggedommen at de gjør noe med det, eller prøver i alle fall å gjøre noe med det. "The Cleanex Project" er et slikt forsøk. Prosjektet er egentlig to prosjekter, hvor den første delen går ut på å skrive programkode som kan implementeres i en Freenetnode for å stoppe nøkler som peker på materiale som inneholder seksuelle overgrep mot barn. Den andre delen av prosjektet går på å finne ut av reaksjonene til brukerne av Freenet i forhold til det å skrive slike programmer som kan fjerne eller blokkere materiale fra Freenet.
The cleanex project fant vi på en side som var lenket til fra "The Freedom Engine" på Freenet. Forfatteren av siden og koden som en kan bruke til å fjerne og blokkere nøkler som peker til overgrepsbilder har fire gode argumenter til hvorfor det er "greit" og ikke går på tvers av verken ytringsfrihet eller filosofien til Freenet. Disse synspunktene er som følger:

4 sitater fra forfatteren:[3]

"Jeg anerkjenner at enhver person har rett til ytringsfrihet slik som den til vanlig er definert, som for eksempel; hvem som helst burde ha rett til å gi ut en avis"

"Men, din rett til ytringsfrihet impliserer ikke at det er min plikt å høre på hva du har å si, for eksempel; jeg trenger ikke lese din avis hvis jeg ikke vil"

"Din rett til ytringsfrihet impliserer ikke at det er min plikt å hjelpe deg å spre ditt budskap til andre, for eksempel; jeg trenger ikke å publisere dine meninger i min avis"

"Det er min ytringsfrihet rett å ikke meddele andre dine synspunkter, for hvilken som helst grunn. Jeg ser ikke på dette som sensur. For eksempel; jeg trenger ikke kjøpe en kopi av din avis og gi den til naboen min slik at han får lest den"

Dette er friske synspunkter som vi burde gi mening til alle advokater av ytringsfrihet og fri sensur, selv på Freenet. The Cleanex Prjoect er ikke av nyere dato, det ble startet 27.07.2003, og er fortsatt oppe å går med siste oppdatering 12.03.2005. Hvilket gir et slags håp.

For å rense den delte katalogen på din node (maskin) så navigerer du deg frem til The Cleanex Project siden på Freenet via for eksempel The freedom Engine, laster ned en fil

[3] http://127.0.0.1:8888/SSK@WP74nrBDes9qDK7dpjiYXYNPl0gPAgM/cleanex/6//
dette er en Freenet adresse

og følger instruksene på siden. Man må skrive noen kommandoer for å installere og aktivere filen, men instruksene er meget enkelt forklart. Programvaren fungerer slik at den blokkerer predeterminerte nøkler som peker til data med innhold en ikke vil være kjent med. Konfigurasjonsfilen kan oppdateres til og blokkerer hvilken som helst nøkkel og en hvilken som helst mengde nøkler. Kildekoden kan man også laste ned slik at man skreddersy dette verktøyet til sine behov. Så langt som vi kan se er dette verktøyet skrevet for Unix/Linux maskiner, og vi vet ikke om dette vil virke på en Windows maskin eller om det finne andre utgaver av dette verktøyet som gjør det. (Forfatteren har ikke gjort seg til kjenne med noe navn og ingen kontakt detaljer så all informasjon om dette verktøyet er hentet fra den siden på Freenet). Opphavsmannen til The Cleanex Project har også snublet over en detalj i kildekoden til programvaren du installerer nå du installerer Freenetnoden på din maskin. Han sier at han ikke kan være helt sikker, men tror at det er en enkel måte å forhindre at overgrepsbilder blir lastet ned til node.

Ideen[4] hans går ut på å utvide "failureTabellen" (som er en del av kildekoden til Fred, som igjen er det du laster ned fra Internet for å installere Freenet på din maskin) til å romme en liste over permanent blokkerte nøkler. Du kan se statistikk fra denne tabellen via en link i det webbaserte brukergrensesnittet til din Freenetnode. "FeilureTabellen" inneholder normalt en liste med nøkler som nylig er blitt spurt etter men ikke ble funnet. Hver gang en spørring etter en nøkkel kommer til din node, sjekker noden denne tabellen for å se om nøkkelen ligger i denne tabellen og hvis den gjør det så avbrytes spørringen umiddelbart. Logikken her er at hvis nøkkelen ikke fantes der for to minutter siden så finnes den sikkert ikke der nå heller og da kastes det ikke bort tid for å sjekke på nytt. For å benytte deg av anti-overgrepsbilder-FailureTable som er inkludert i Cleanex verktøyet som du kan laste fra The Cleanex Project siden på Freenet må du inkludere den nedlastede filen før Freenet.jar i CLASSPATH i din node. Så må du starte noden din (Freenet) på nytt. Du kan sjekke om det virker ved å gå til Failure Table Stats fra det webbaserte brukergrensesnittet. På toppen av den siden skal det da stå to nye linjer; "Permanently Blocked" og "Number of Hits on Perm Blocks"

Som forfatteren selv sier; "Jeg vet ikke om dette er et fullgodt og effektivt tiltak og jeg anbefaler du kjører (starter) Cleanex regelmessig". Alle monner drar sier vi og er glad for at det faktisk er noen der ute som gjør en innsats! Dessverre er dette "Cleanex Project" det eneste vi har funnet på Freenet som aktivt tar et ansvar for å gjøre noe med spredningen av overgrepsbilder på Freenet, men det betyr ikke at det ikke er flere lignende prosjekter der ute. Og det betyr også at det er mulig for alle som innehar en Freenetnode å hindre spredningen av overgrepsbilder i Freenet. Slik at alle som vil være med på å verne om våre barn, og allikevel støtte opp om ytringsfrihet og de demokratiske prinsipper i et hvilket som helst nettverk kan gjøre det. Vår takk og ros til forfatteren av "The Cleanex Project", hvem han eller hun måtte være. Nå skal det sies at det som er forklart ovenfor kan virke en smule teknisk, og det er vi enige i, men det er slik med ny teknologi at hvis man skal kjempe på frontlinjen i en krig er mye nytt og uoppdaget land, man må være villig til å sette seg inn i nye ting på en daglig basis og det samme gjelder her. Freenet er en ny teknologi, som åpner mange nye dører for alle impliserte, inklusive

[4] http://127.0.0.1:8888/SSK@WP74nrBDes9qDK7dpjiYXYNPl0gPAgM/cleanex/6//
dette er en Freenet adresse

oss som kjemper mot produksjon, distribusjon og bruk av overgrepsbilder, og ikke minst dem som benytter seg av det. Poenget er at det finnes midler vi kan bruke, eller sagt på en sterkere måte; våpen vi kan bruke i krigen. La oss finne ut av det!

Sporing av overgrepsbilder i Freenet

At det finnes overgrepsbilder på Freenet mener vi altså er et faktum, eller i alle fall ikke usannsynlig i forhold til de få observasjoner vi har gjort i forhold til lenkenavn inne på flere portaler. Videre mener vi at det er udiskutabelt at man trenger tiltak for å spore de som driver med dette. Krigen mot overgrepsbilder er en av få kriger det alltid er verdt å utkjempe. Men som vi har oppdaget gjennom vår forskning i Freenet kan det vise seg at dette blir vanskelig om ikke fullstendig umulig, i et så kryptert miljø som det vi finner her.

Den første teorien vi så på var å spore IP adresser i nettverket. Dette viste seg å fremkalle flere tekniske problemer. For det første sitter alle Freenetnoder bak en proxyserver som bruker adressen 127.0.0.1:8888, og dermed maskerer IP adressen. Dette er ikke det verste problemet å overkomme siden all trafikk som foregår på Internet går gjennom en ISP (Internet Service Provider) og her er det mulig å plukke opp IP adresser. For det andre kan man bare spore IP adressen til en som laster ned en fil frem til den første noden i nettverket og ikke helt frem til den noden som eventuelt har filen man prøver å laste ned. Fordi når en spørring sendes ut på Freenet så går den fra maskinen som sender spørringen og til den nærmeste logiske noden i nettverket i henhold til routingtabellen, så overtar den noden spørringen og sender den videre som sin egen, og slik fortsetter det til spørringen gir resultat eller HTL dør ut. Det samme skjer når en skal spore hvor en fil kommer fra, det er kun den nærmeste noden man kan se adressen til og det trenger ikke være opphavet til filen.

Så tenkte vi at man kan forsøke å ta en og en node i nabolaget ved å sette HTL på spørringer ned til 2 slik at søket gikk til kun en' node utenfor ens egen, og hvis det gav resultat er i form av overgrepsbilder gikk det an og samarbeide med ISP om å få overvåket denne nodens IP eller eventuelt ta beslag i maskinen som noden er satt opp på. Problemet her går ut på at filene i den delte katalogen er kryptert slik at eieren av den katalogen trenger ikke vite at den inneholder overgrepsbilder, og trenger slettes ikke være den som har produsert eller publisert dem. Man ville sannsynligvis kaste bort store mengder penger og tid på å beslaglegge maskiner som ellers er “rene”. Siden filer som blir etterspurt sprer seg på nærliggende noder i nettverket blir denne fremgangsmåten kanskje ikke den beste. Men man ville i alle fall fjerne noder i Freenet som har overgrepsmateriale i den delte katalogen.

Vi bør utforske alle tenkelige tiltak, og i forbindelse med beslag er det et par ting som bør nevnes. Hvis en person benytter seg av overgrepsmateriale via nøkler som han eller hun har fått fra en annen person så er disse nøklene så komplisert at det vil være nesten umulig å huske en', langt verre å huske flere.

La oss illustrere det ved et eksempel på en nøkkel som er lagt opp som URL i et Freenet webgrensesnitt: http%3a//127.0.0.1%3a8888/SSK@rBjVda8pC-Kq04jUurIAb8IzAGcPAgM/TFE//.

Da kan man jo spekulere i hvor disse personene oppbevarer disse nøklene. Lagrer de sine nøkler i en katalog på maskinen sin eller blir de skrevet ned på en lapp som blir lagt i lomma?

Hvis man finner nøkler på en beslaglagt maskin er nærliggende å tro at disse er brukt av misstenkte, og hvis man da gjør et søk med disse nøklene som har HTL satt til 1, så vil man se om disse nøklene refererer til overgrepsmateriale i den lokale delte katalogen på mistenktes maskin. Hvis dette er tilfelle så er det klart som dagen at vi har å gjøre med en som benytter seg av og er med på å spre overgrepsmateriale. Man kan også benytte disse nøklene til å søke etter overgrepsmateriale på andre nærliggende noder, ved å bruke HTL lik 2 for eksempel, men det er en del faremomenter ved dette som vi kommer tilbake til om litt. Hvis man bruker en nøkkel og HTL lik 2 så vil spørringen gå ut til kun en node og så dø, hvis den ikke fant noe. Spørringen kan kjøres til man finner noe eller jorden går under.

Når man eventuelt finner noe med denne nøkkelen som man vet peker på overgrepsmateriale, og har brukt HTL lik 2 , da vet man at man kan spore seg frem til den maskinen hvor dette materialet befinner seg siden det da ikke er noen noder mellom oss og kildenoden. Disse krypterte nøklene er ikke beskyttet på noe vis, med egne passord eller lignende, det vil si, det går selvfølgelig an å kryptere allerede krypterte filer, så det er mulig å passordbeskytte en slik nøkkel for utvidet sikkerhet. Så hvis det tas beslag i maskiner er det en av tingene politiet bør lete etter. Videre så har man en egenskap ved det webbaserte brukergrensesnittet, som er en bokmerkeside, hvor brukere av Freenet lagrer sine favorittsider, eller nøkler. Her kan det også være ting å hente hvis det ligger lenker (nøkler) til sider med overgrepsmateriale der så kan også med en rimelig stor grad av sikkerhet si at man har med en bruker og spreder av overgrepsmateriale å gjøre. Det med passord i forbindelse med nøkler på Freenet er noe som enkeltpersoner i så tilfelle gjør lokalt på sin maskin. Det er ikke noe mekanisme i Freenet for passordbeskyttelse av materialet eller nøklene som peker til materialet.

En egenskap ved datamaskiner og software generelt fører til den neste delen i forbindelse med et beslag. Når man laster ned en fil fra Freenet, eller fra Internet for den saks skyld, så må denne filen åpnes i riktig program får at man skal kunne se på innholdet. En tekstfil åpnes i en teksteditor, et regneark i f.eks. Excel og et bilde i et bildevisningsprogram som Picture viewer. Slik at hvis en lastet ned et overgrepsbilde til sin maskin så gjør man lite med det hvis det er kryptert, og slik er det faktisk ikke når man laster ned bilder fra en side på Internet. Bildene man laster ned blir lagret til en selvbestemt plass på harddisken og gitt navn etter ønske. Formatet på disse bildene er som oftest jpg eller jpeg, og hvis du laster ned overgrepsbilder fra Freenet eller Internet, så er det ofte disse formatene bildene blir lagret i, og de blir ikke kryptert når du lagrer dem til din harddisk. Bildene vil være kryptert mens de er på tur til din maskin, slik er det i Freenet, men så snart du har lastet ned bildet og ser på det på skjermen, så kan du klikke på det og lagre det på maskinen.

Det som skjer da, i forhold til Freenet er at du laster ned bildet fra din egen node til din egen harddisk.

Det kan være litt vrient å skjønne dette siden alt i denne sammenhengen foregår på din maskin. Kort forklart skjer følgende; Du ber om å få se en side på Freenet, ved å for eksempel klikke på en lenke i en portal. Denne siden blir så transportert til din maskin og lagret i den delte katalogen. Derfra blir siden vist på din skjerm og herfra kan du lagre bildene til en katalog på din maskin, for eksempel Mine Dokumenter i Windows.
Det at filene er kryptert i transitt mellom nodene henger litt sammen med at Freenet noden din bruker en proxyserver til å sende og motta filer, og disse filene blir lagret i den delte katalogen og vist fra denne proxyen til du lagrer dem på maskinen din ved å klikke på bildene og trykke lagrer. Ikke bare blir bildet lagret på din maskin da, men det blir også vanskelig å fjerne. Man trenger spesiell kunnskap og programvare for å permanent og uopprettelig fjerne filer fra en harddisk. Så har man lastet ned overgrepsmateriale og lagret dette, så er stort sett sannsynligheten for at det finnes på disken meget stor selv om man har slettet filene. Vi kan legge til at så lenge du ikke klikker på noe og lagrer det, men bare lukker siden du ser på så vil all informasjon på den siden forbli i den delte katalogen og forbli kryptert.

Et annet problem med dette å laste ned overgrepsmateriale for å spore kilden eller de som har det i den delte katalogen er av en meget alvorlig natur. Dette går på spredningen som skjer når man prøver å laste ned filer fra Freenet. I det du forsøker å laste ned et overgrepsbilde så er du automatisk med på å distribuere det samme bildet. Og hvis din spørring har en HTL på 25, og du får napp på node nummer 24, så vil nok det bildet bli lagt igjen på 23 maskiner før det kommer til din maskin. Denne problemstillingen fant vi da vi tenkte i de baner at man kunne laste ned materialet og analysere det for å så kunne identifisere personer eller andre detaljer på bildene og så gå til aksjon i forhold til det man fant. Dette er altså ikke å anbefale på noe vis. Hvis politiet mener at det er en pris som må betales for å komme vederstyggeligheten til livs så får politiet ta den avgjørelsen. Men vår oppfattning er at man faktisk bare ville gjøre vondt verre, siden spredning gjør tilgangen enklere for dem som er på jekt etter slikt materiale.

Omvendt tenkte vi at man kunne sette opp en node og publisere filer som man utgav for å være overgrepsbilder med en HTL på 1, slik at filene kun blir publisert til den delte katalogen på den noden man satte opp. Så kunne man spore de maskinene som sendte spørringer etter dette materialet, men også da kun den første maskinen i kjeden, som selvfølgelig ikke trenger være den som faktisk har sendt spørringen, og problemet består. Ett annet problem her ville jo da bli distribusjon av nøklene til denne siden eller de filene og det at når folk der ute finner ut at disse nøklene er ”falske” vil de snart bli forkastet. Problemet med at så snart noen spør etter materiale fra den noden så blir det materialet predt utover på Freenet kan også føre til at man til slutt ikke fikk så mange spørringer fordi disse vil gå til andre noder som da har fått en kopi av alt vi måtte legge ut på vår noe.

Et annet problem med å finne ulovlig materiale i en delt katalog på en eventuelt beslaglagt maskin er krypteringen. Det brukes opptil 256 bits kryptering på all data som trafikkerer Freenet og som lagres i den delte katalogen. Det vil kreve mye tid og datakraft for å bryte krypteringen, og som vi har vært inne på tidligere blir filer som ikke blir mye etterspurt til syvende og sist overskrevet. Dette kan føre til at man går glipp av å finne ulovlig materiale på en maskin som man har mistanke om inneholder dette hvis man ikke er raskt nok ute med et beslag. Vi har tenkt på infiltrering av chatterommene på Freenet for å angripe overgriperne den veien, men det er vår oppfattning at det kan bli vanskelig i beste fall.

Det kan være at de som driver med overgrepsbilder kanskje utveksler personlig informasjon om seg selv, dette vet vi ingenting om, men hvis det er tilfelle så kan det kanskje være til hjelp for politiet. Vi har et sitat hentet fra en av lenkene på siden “The Freedom Engine”, lenken er som følger; Portrait of a Phedophile, og det sitatet under lenken er som følger; “I was stupid enough to send my personal information on a pedo board”, og direkte oversatt til Norsk blir det: “Jeg var dum nok til å utlevere personlig informasjon i et chatterom for pedofile”, så vi antar at folk som driver med dette, og som prater med hverandre i disse chatterommene, er meget forsiktig med hva de utleverer om seg selv. Dette er en antagelse basert på ett sitat fra ”en mann på en side”, men vi synes den sier sitt. Vi nevner at vi ikke har vært inne på den siden for å se på innholdet, men antar at det dreier seg om anger i forhold til å bli tatt av politiet på bakgrunn av å ha utlevert personlig info. Det kan også være at denne personen er blitt hengt ut med navn og adresse av andre som ikke liker det han drev med, men som sagt, det blir kun spekulasjoner. Det vi vil frem til med dette er at de som driver med dette er nok forsiktige, og med tanke på infiltrering så kan denne “forsiktigheten” gjøre det vanskelig for politiet. All trafikk inne på disse chatterommene er også selvfølgelig kryptert, hvilket vil by enda mer vansker for politiet.

Hvem bruker Freenet?

Dette blir i beste fall en kvalifisert gjetting, men det er vår oppfattning at Freenet ikke er kommet så langt i sin utvikling at det er noe den menige mann i gata kommer til å benytte seg av i stor utstrekning med det første. Det er flere grunner til dette. For det første er Freenet vanskelig å stille inn etter installasjon slik at virker best mulig i forhold til ditt bruk. For det andre er Freenet meget tregt, sidene bruker evigheter på å laste, fra flere minutter til flere timer, og ofte aldri.

Det er tilsynelatende komplisert med alle disse nøklene når man skal publisere og hente filer fra Freenet og man kan ikke søke etter filer. Man kan søke etter spesifikke nøkler, med det gir jo egentlig lite mening. I forhold til Kazaa som er en klient i Gnutella nettverket så vil nok de fleste som bare laster ned litt musikk, film og tekstfiler med innhold som er allment akseptert velge Kazaa, eller en hvilken som helst annen P2P nettverksløsning fremfor Freenet. Det er vårt inntrykk at de fleste som kommer til å benytte seg av Freenet er de som har noe å skjule, og dermed trenger all den sikkerheten som Freenet tilbyr. For den vanlige Internet bruker vil nok de andre fildelings applikasjoner der ute være å foretrekke.

FTP har i en årrekke vært flittig brukt og vil nok ikke dø med det første som en konsekvens av Freenet, selv om Freenet skulle vokse seg mye større enn det er i dag og i tillegg bli raskere og søkbart. Det samme gjelder nok de fleste andre fildelings-applikasjoner der ute. Til og med IRC med fildelingsserver kommer nok til å bestå i enda noen år.

Som de fleste som prøver Freenet vil finne ut er det svært vanskelig å finne spesifikke ting man er på jakt etter. På grunn av det ikke går an å søke på filnavn blir det en tidskrevende jobb å finne frem til akkurat den filen eller den artikkelen man er på jakt etter. Dette blir ikke lettere med at Freenet vokser. Internet er gigantisk i forhold til Freenet, som er beskrevet som et "Internet i Internet", men der ute har man f.eks. Google, som finner alt du er på jakt etter i løpet av sekunder. Så hvorfor bruke Freenet da? Hvis du er på jakt etter ulovlige data, og er redd for konsekvensene det å laste ned slikt fra Internet kan medføre, ja da tar du deg sikkert tid til å sette deg inn i å bruke Freenet. Men vi tror dette "Internet i Internet" er for spesielt interesserte og for de som holder på med lyssky aktiviteter. Vi vil ta med her at det absolutt finnes en mulighet for at det kan være en og annen kineser som får sagt sitt via Freenet, men vi frykter at han neppe blir hørt i særlig grad.

Hvem er forbrukeren av overgrepsbilder?

Hvem som benytter seg av overgrepsbilder er ikke lett å si noe om fordi vi finner pedofile i alle land, alle samfunnssjikt og klasser. Det som har kommet frem under nyere forskning på det med overgrepsbilder på Internet er at flere og flere benytter seg av denne type materiale fordi den "vanlige" pornoen ikke er tilfredsstillende nok..

Sitat:[5]
...With this hobby we get bored after a while with the usual and we risk a bit to get new stuff or actual experience. It's a natural progression. Like stealing. You start small. Get bored. Go for bigger stuff....

Kan hende det er en iboende egenskap hos mennesket, dette at vi stadig vil se nytt og råere materialet. Vi har jo kommet så langt, i alle fall de aller fleste av oss, at vi ser nyhetene på TV og spiser middag samtidig. Selv om nyhetene bare inneholder krig, drap og elendighet. Kanskje blir vi avstumpet med tiden og for å stimuleres så må det kraftigere, eller rettere sagt nyere krutt til for å gjøre det. Hva dette sier om den gjennomsnittlige bruker av overgrepsbilder kan diskuteres, men at flere og flere benytter seg av det er nok kanskje riktig. "Flere og flere" er kanskje en litt vel løs påstand, siden vi ikke har noe empirisk materiale å basere vår antagelse på, men det er jo inntrykket vårt etter materiale fra Redd Barna og NyeKRIPOS.

Som oftest er det menn som benytter overgrepsbilder, og ofte menn over 20 år, og som oftest blir disse klassifisert som pedofile på bakgrunn av deres handlinger. Flere hevder at

[5] http://www.media.uio.no/mediert/artikler/2000/2000nr1/2000nr1s14.html

dette med pedofili er en type seksuell legning på lik linje med heterofili og homofili, og om det er tilfelle eller ikke skal vi ikke debattere her. Det vi derimot skal si noe om er at hvis man blir klassifisert som pedofil på bakgrunn av at man er blitt arrestert for å ha benyttet seg av overgrepsbilder, så er det nok tenkelig at vi vil få flere pedofile inn i samfunnet som ”nettopp” har konvertert.

Men tilbake til utgangspunktet, hvem er forbrukeren av overgrepsbilder. Den gjennomsnittlige bruker av denne type materiale er trolig mann, hvit og over 20 år, jobber med hva som helst, bor hvor som helst, gift eller ugift. Det er vår oppfattning at det kan være hvem som helst. Vi vil her legge til at vi på ingen måte er kvalifisert til å gi noen vitenskapelig formening om dette, så dette er bare antagelser fra vår side.

Tekniske aspekter ved Freenet

Fred

Fred står for Freenet Reference Deamon. Det er programvaren som kjøres når du starter opp Freenet. Fred er din Freenet node, som tjenestegjør som router, datacache og personlig gateway til Freenet. For å kjøre krever fred at en konfigurasjonsfil er opprettet, noe som gjøres automatisk under installasjonen. Fred har ikke noe grafisk brukergrensesnitt. Til vanlig kommuniserer du med fred gjennom det webbaserte brukergrensenittet (http://127.0.0.1:8888).[6]

Installering

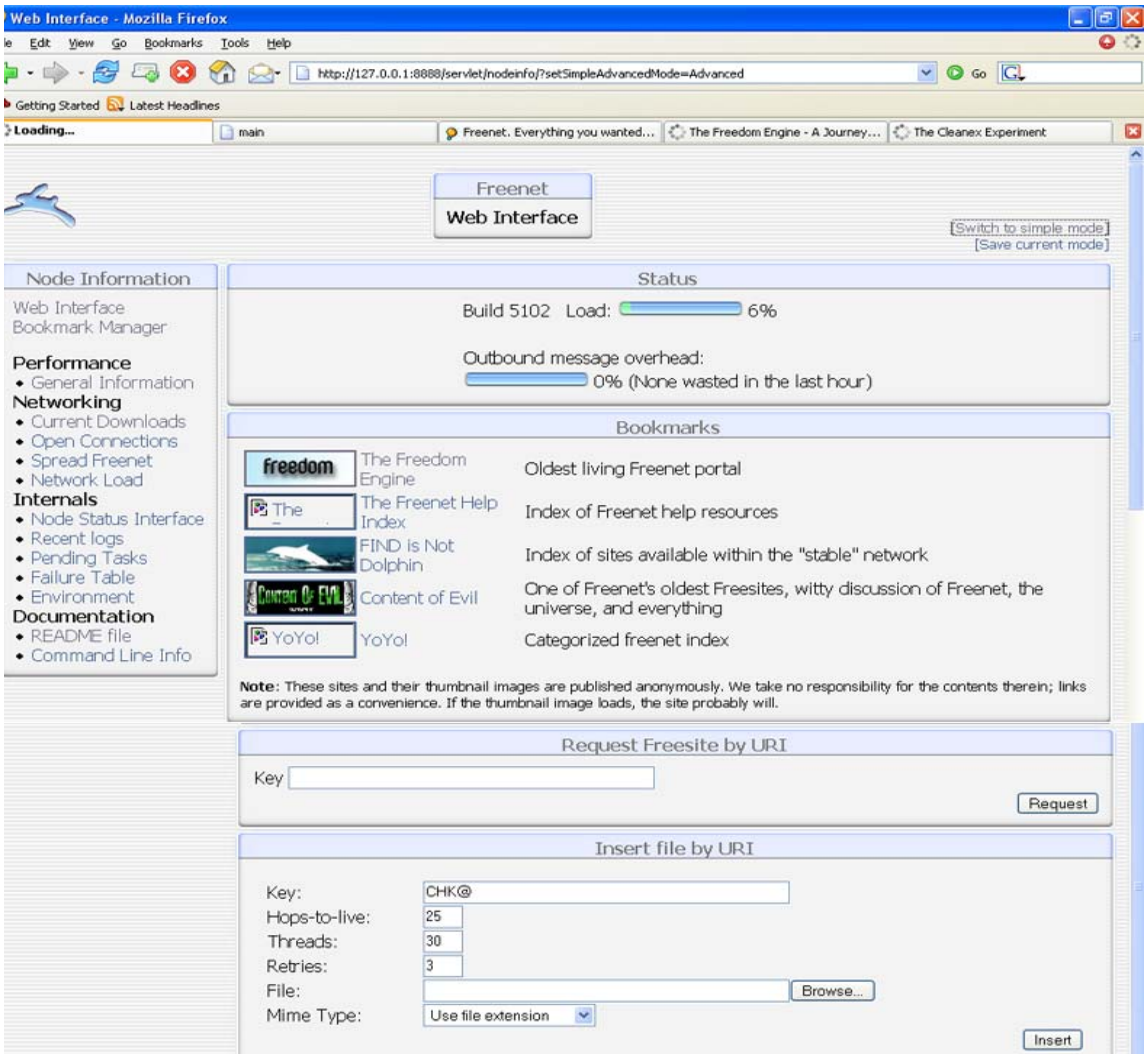
Når du bestemmer deg for å bli Freenet bruker må gjennom to små enkle steg. For det første må du laste ned innstallesjonsprogramvaren og så må du følgelig installere den på din maskin. En ting du må passe på er at du har Java Runtime Environment versjon 1.4.1 eller høyere på maskin. Hvis ikke velger du bare å laste ned Freenet med Java fra den nedlastningssiden du måtte bruke.
En slik side er; http://Freenetproject.org/index.php?page=download
På denne siden får du tre valg i forhold til hvilken utgave du skal laste ned. Du kan velge mellom Freenet for Windows med eller uten Java og Freenet for Unix/Linux. Når du har lastet ned filen er det bare å kjøre installasjonsfila som ved installasjon av et hvilket som helst annet program. Installasjonsprogrammet kobler seg under installasjon opp mot nett og laster ned to større filer, og du får valget om du vil laste en fil som heter seednodes.ref under konfigurasjons delen av installasjonen. Når programvaren er ferdiginstallert ender du som regel opp med startmeny elementer, et ikon på skrivebordet, og en katalogstruktur i programfiler (Windows). For å starte Freenet er det bare å klikke på ikonet på skrivebordet. Da starter du din Freenet node og denne blir markert som et lite ikon nede til høyre på startlinjen, (ved siden av klokken). Dobbeltklikk på dette ikonet og du åpner det webbaserte brukergrensesnittet som er ditt vindu ut mot Freenet akkurat slik Internet Explorer eller Mozilla med startsiden www.startsiden.no er ditt vindu mot Internet.

Webbasert brukergrensesnitt

Det webbaserte brukergrensesnittet du får opp i nettleseren din når du starter Freenet er i realiteten ikke mer enn en HTML kodet nettside (som en hjemmeside) til din Freenet node. Det er også vinduet ditt ut mot resten av Freenet. Dette webbaserte brukergrensesnittet inneholder flere sider som kan aksessers vi lenker på forsiden. Det er to moduser til denne siden, enkel og avansert. I enkel modus har du tilgang til 5 lenker som peker direkte til andre sider på Freenet. Disse er per i dag The Freedom Engine (en portal), The Freenet Help Index (en freesite med hjelp i forbindelse med Freenet), FIND is not Dolphin (en portal), Content of Evil (freesite med diskusjon om Freenet, universet og alt) og YoYo (en portal).

[6] https://Freenet.homelinux.net:4433/servlet/nodeinfo/documentation/cli

Du har to status indikatorer som forteller deg hvor mye båndbredde som er ”bortkastet” den siste timen og load, som forteller om størrelsen på trafikken mot di node. I tillegg til dette har man flere lenker til de andre sidene. Disse er sidene er; Bokmerker, Read me, spre Freenet, nedlastninger og generell informasjon.
Hvis du bytter til avansert modus får du i tillegg opp; Node status Interface, Recent Logs, Pending Tasks, Failure Table, Environment og Command Line Info. Du får også opp to utvidede funksjoner. Den e er en søkefunksjon hvor du kan skrive inn en nøkkel og så lete etter den på Freenet. Og en opplastningsfunksjon hvor du kan velge en fil du vil laste opp, stille inn HTL og annen informasjon og laste opp filen til Freenet. Under finner du et bilde av det webbaserte brukergrensesnittet.



Slik ser det webbaserte brukergrensesnittet ut når du åpner det etter å ha startet Freenet. Vi beklager den dårlige billedkvaliteten. Som du ser har du status øverst, lenker til andre Freenet sider i midten, nøkkelsøking og filopplasting nederst og lenker til andre sider i brukergrensenittet til venstre. Dette er et bilde tatt av brukergrensesnittet i avansert modus.

Datastore (delt katalog)

Når man installerer Freenet på sin maskin opprettes det en katalogstruktur i programfiler katalogen (Windows) hvor alle filer som har med Freenet blir installert. I denne katalogstrukturen opprettes det en katalog som heter ”store”. I likhet med andre P2P nettverk er litt av hensikten å dele file med andre på nettverket og man ”offerer” en viss mengde harddiskplass til dette formålet. Katalogen ”store” er Freenets svar på den delte katalogen. Det er her filene om deles på nettverket blir lagret. Nå er det i midlertidig slik med Freenet at du ikke har kontroll på hvilke filer som blir delt fra din maskin, slik som du har med for eksempel Kazaa og Limewire.

Filene som blir lagt i den delte katalogen i forbindelse med Freenet er kryptert slik at du faktisk ikke kan vite hva som befinner seg der. Dette på grunn av Freenets iboende arkitektur og ikke minst i tråd med tanken bak Freenet; publisering under full anonymitet. I tillegg er disse filene kryptert for å beskytte eieren av noden mot det eventuelt ulovlige materialet som måtte befinne seg der som et resultat av resten av trafikken på Freenet. Det er nemlig slik med Freenet at hvis din node står mellom to noder som kommuniserer med hverandre og sender data mellom hverandre, så blir alle filer som de utveksler lagre på din maskin hvis dere datastrøm blir routet den veien. Vi kommer tilbake til routing litt senere i rapporten.

Størrelsen på denne katalogen varierer i forhold til ledig plass på din harddisk når du installerer Freenet på din maskin. Denne størrelsen kan endres etter installasjon. Det er ikke slik med denne delte katalogen som blir et resultat av en Freenet installasjon at du bare kan putte filer du vil dele med andre i den. Det er litt mer komplisert enn som så. Men det er i aller høyeste grad mulig, om det har noen hensikt skal vi kommentere om litt. Hvis du vil legge filer inn i den delte katalogen på din maskin kan laste opp en fil via det webbaserte brukergrensenittet og sette HTL lik1. Da vil disse filene dine kun bli publisert til den delte katalogen på din maskin.

Og så kan en jo spørre seg om det har noe for seg i det hele tatt. Svaret er i de aller fleste tilfeller; selvsagt ikke. På grunn av at de som eventuelt skal laste ned disse filene du så gjerne vil dele trenger den offentlige nøkkelen som ble laget da du publiserte filene for å få lastet de ned. Litt av tanken bak Freenet er jo nettopp å spre materialet til så mange noder som mulig, det gjøres under publikasjon ved å sette en høyere HTL, normal ca 20. Dette vil også føre de filene du vil dele med resten av Freenet også blir lettere tilgjengelig for de som vil laste dem ned. I etterforsknings øyemed kan nok dette med å laste opp filene til kun sin egen node for så å forsøke å spore de nodene som forsøkte å laste ned materialet etter at nøkkene var publisert. Dette vil vi komme tilbake til senere i rapporten. For å oppsummere; når du installerer Freenet på din maskin opprettes det en katalog som delte filer blir lagret i. Alt innholdet i denne katalogen er kryptert.

Fproxy

Fproxy er en webserver som blir installert samtidig som du installerer Freenet på din maskin og den virker som anonymitetsfilter. Det er denne webserveren som tar seg av all trafikk mellom din maskin og Freenet. Fproxy blir satt opp på lik linje med Apache og får adressen localhost eller 127.0.0.1 og en eventuell port hengt på bak adressen. Vanligvis 8888, og adressen til fproxy blir da seende slik ut; http://127.0.0.1:8888. Du kan selv stille inn hvilken port fproxy skal lytte til. Når du åpner det webbaserte brukergrensesnittet til Freenet blir adressen i adresselinja i nettleseren din seende slik ut: http://127.0.0.1:8888/servlet/nodeinfo/?setSimpleAdvancedMode=Simple
Når du klikker på en lenke ute på Freenet vil fproxy laste ned siden for deg og dermed er det IP adressen til fproxy som blir brukt i den trafikk sammenhengen. Det er dette som gjør fproxy til et anonymitetsfilter.

Noder

Ordet node kommer fra det Latinske ordet ”Nodus” som betyr knute. I følge Oxford English Dictionary betyr node også ”en komponent i et datanettverk”, og den siste beskrivelse passer bra i denne sammenhengen. I Freenet er en node enkelt og greit en datamaskin som har installert Freenet programvaren og er koblet opp mot Freenet via Internet. En node i Freenet kan også beskrives dom programvaren installert på en maskin som er koblet opp mot andre maskiner med samme programvare installert. En Freenet node har tre hovedkomponenter på programvare siden. En delt katalog (eng. datastore), et webbasert brukergrensesnitt og en proxyserver. Hele noden blir styrt av programvaren Fred, som er beskrevet tidligere. Noden inneholder i tillegg krypterings programvare.

Nøkler

Nøkler er et begrep hentet fra kryptografi og bruken av disse kan kanskje beskrives slik: Når du skal sende et dokument over Internet, et dokument som for eksempel en e-post, som du ikke vil at noen skal kunne lese, bortsett fra mottakeren. Så kan du putte denne e-posten i en safe (pengeskap med kodelås) og så sende hele safen (pengeskapet) til mottaker. Disse nøklene vi snakker om fungerer som koden for å åpne pengeskapet. Dette impliserer at mottaker må ha koden for å få åpnet penge skapet og dermed få lest e-posten.

Det fines to hovedtyper av nøkler I bruk I Freenet I dag. Denne ene heter CHK (Content Hash Key) den andre SSK (Signed Subspace Key).

En CHK er en SHA-1 hash av et dokument og dermed kan en node sjekke om det dokumentet som blir levert er det riktige ved å hashe det og så sjekke det opp mot nøkkelen. Denne nøkkelen inneholder ”kjøttet”, eller dataene i filene som publiseres på

Freenet. Den bærer med seg alle binære data blokker for innholdet i en gitt fil tilbake til den noden som har spurt etter filen for sammensetting og dekryptering. CHK nøklene er unike av natur og brukes for å forsikre at innholdet som nøkkelen peker til ikke kan forandres på sin ferd i Freenet. Hvis en fiendtlig innstilt node (les; den som styrer noden) forandrer på innholdet i en fil under en CHK nøkkel vil dette umiddelbart bli oppdaget av den neste noden i hierarkiet, eller klienten. CHK nøkler bidrar også til å unngå redundans siden alle CHK nøkler er unike og følgelig innholdet under dem.

SSK nøkler er basert på public-key-cryptography. For tiden bruker Freenet DSA systemet som sin public key infrastruktur. Dokumenter som blir publisert under SSK nøkler blir signert av den som publiserer og denne signaturen kan verifiseres av hver node for å forsikre at dataene i filen ikke har blitt klusset med. SSK nøkler kan brukes til å etablere en verifiserbar identitet på Freenet. I tillegg gir dette den som publiserer dokumenter muligheten til trygt å kunne oppdatere det som blir publisert under nøkkelen. En undertype av SSK nøklene er Keyword Signed Key, eller KSK, hvor nøkkelparet blir generert på en standard måte fra en menneskelig lesbar tekststreng. Publikasjon under KSK gjør at dokumentet kun kan lastes ned og dekrypteres hvis den som laster ned filen kjenner til den menneskelig lesbare tekst strengen. Dette gir en enklere URI å referere til, men med mindre sikkerhet.

Routing

Freenet bruker en kombinasjon av nøkkelbasert routing og det som kalles en distribuert hash tabell (DHT). Egentlig er det strengt tatt nøkkelbasert routing som Freenets routing protocoll er bygd på. Nøkkelbasert routing (key based routing KBR) er en applikasjons programmert brukergrensesnittbasert nettverk routing metode som bruker krypterte nøkler. Routing metoden til et nettverk spesifiserer hvordan, når og til hvem data blir overført. Krypteringsnøkkelen blir bruk til å kryptere data som sendes, men kan også brukes til å hente tilbake data. Dette kalles en API (Aplication Programming Interface) og er ett sett med definisjoner som gjør at en type programvare kan snakke med en annen. Nettverks routings metoden er en del av ett nettverks arkitektur. Metoden spesifiserer som sagt hvordan data overføres. Noen nettverk kan ha flere enn en routing metode, til og med en kombinasjon ev flere. I kryptografi er kryptering en prosess som brukes til å forkle informasjon slik at den blir uleselig uten spesiell kunnskap om hvordan. Sterk kryptering ble født på 70'tallet og blir brukt i flere sammenhenger i dag, som for eksempel på Internet, e-post, mobiltelefoni, og minibanker.

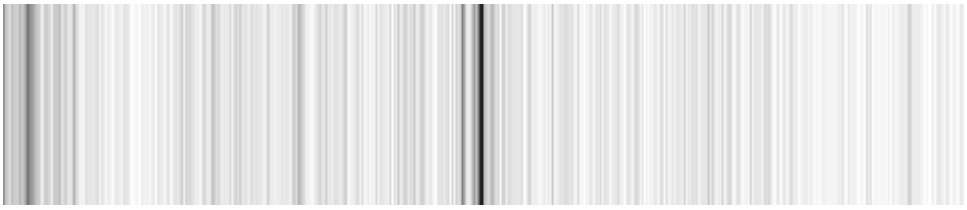
Så over til Freenets spesifike routing system. Selv om Freenets routing mekanisme ble utviklet uavhengig, så har den flere likheter med den som brukes i distribuerte hash tabeller. Den store forskjellen er at Freenet sine noder ikke har statiske spesialiseringer, og at routing algoritmen er heuristic[7] av natur. Derfor så er det ingen garanti for at denne algoritmen vil finne en gitt bit med data på nettverket.

[7] http://dictionary.reference.com/search?q=heuristic

Slik fungere routingen på Freenet per i dag. Enhver node i Freenet nettverket er pålagt å utføre en enkel tjeneste for andre noder i nettverket. Når en node mottar en spørring mot en bestemt nøkkel, så gjør denne node sitt beste for å finne data som passer til den nøkkelen så raskt som mulig og så sende denne data tilbake til den noden som spurte etter dataene. Så fremt at alle noder i nettverket gjør denne oppgaven tilfredsstillende så vil Freenet virke som planlagt. I det enkleste tilfellet vil den noden som får en spørring ha dataene det spørres etter lagret lokal i sin delte katalog (datastore), og umiddelbart sende disse tilbake til den noden som spurte etter dem. I de fleste tilfeller, derimot, vil noden bli nødt til å spørre videre på nettverket, spørre neste node som den tror vil være best skikket til å hente de data som det er snakk om. Måten Freenet avgjør dette på er kjernen i Freenet algoritmen.

Per i dag så er algoritmen som brukes til å velge hvilken node som skal spørres etter en gitt nøkkel relativt enkel. Kort forklart; når en node videresender en spørring for en gitt nøkkel til en annen node i nettverket, og den noden finner de data det er snakk om, så blir adressen til ”upstream” noden (muligens den noden hvor de aktuelle data befant seg) lagret og inkludert i svaret som sendes nedover hierarkiet, dette blir kalt datakilden (DataSource). Noden som sendte spørringen videre lagrer den nøkkelen som ble spurt etter og datakilden som kommer tilbake som svar. Det er antatt at en upstream node er en grei plass å route fremtidige spørringer som ligner den siste spørringen. Det kan man sammenligne med at hvis din venn Petter visste svaret på et spørsmål om Frankriket, så er det sannsynlig at han vet svaret på et spørsmål om Belgia.

Til tross for sin enkelhet, har denne metoden vist seg å være overraskende effektiv både i simuleringer og i praksis. En forventet bieffekt av denne fremgangsmåten var at noder ville ha en tendens til å spesialisere seg på å hente data knyttet opp mot en spesiell type nøkler og ikke bry seg om enkelte andre typer. Dette blir nesten som en spesialisering blant folk, noen er snekkere, andre er bakere. Denne effekten har blitt observert i fysiske noder i Freenet. Bildet under viser en representasjon av nøkler som er lagret i en gitt Freenet node:



X aksen representerer nøkkelrommet (nøkkelvolumet, eng. Keyspace), ytterst på venstresiden er nøkkel 0, ytterst på høyre side er nøkkel 2 opphøyd i 160. De mørke områdene indikerer hvor noden ”vet bedre”, det betyr at hvor de mørke stripene befinner seg så har noden god informasjon om hvor den skal route spørringer i forhold til de nøklene.

Legg merke til at når noden først ble opprettet ville nøkler ha vært jevnt fordelt utover ”nøkkelrommet”. Dette er en indikasjon på at Freenets routing algoritme fungerer som den skal. Noder spesialiserer seg slik på bakgrunn av en oppbyggende feedback effekt.

Når en node svarer med suksess på en spørring til en gitt nøkkel, øker det sannsynligheten for at andre noder vil route liknende spørringer dit i fremtiden. Og over tid dukker den spesialiseringen opp som vi kan se på bildet over.

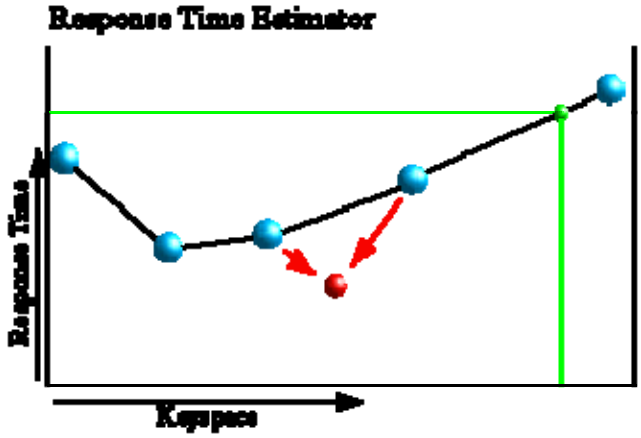
Neste generasjons routing mekanisme.

Det at noe virker betyr ikke at det ikke er rom for forbedringer. På det enkleste nivået så kan man merke seg at dagens algoritme ikke skiller mellom en treg node som sitter bak et modem og en rask node som sitter bak en bredbånds forbindelse.. I tillegg er det slik at å teste hvordan den nåværende algoritmen oppfører seg er ved hjelp av simuleringer eller ved å observere fysiske noder på det virkelige nettverket. Dette fører til en langsom utviklingsprosess. Ved å bruke den informasjonen som er tilgjengelig for en Freenet node kan det bli gjort dramatiske forbedringer i en nodes routings muligheter som vil gjøre at en node kan route mye raskere. Ved å unngå gjetting, og heller nærme seg en basis i statistisk virkelighet, kan man akselerere utviklingen ved å observere effektivitetsøkningen ut fra forandringer på en enkelt node før den blir satt ut i livet. Dette er hva den neste generasjonen med routing skal adressere.

Kjerneideen bak designet på neste generasjons routing er å gjøre nodene i Freenet smartere når det kommer til å avgjøre hvor informasjon skal routes. For enhver nodereferanse som er lagret i routing tabellen vil en node samle utfyllende informasjon om disse. Denne informasjonen inkluderer responstider for spørringer mot spesifikke nøkler, antallet heldige spørringer, og tiden det tar for å opprette en tilkobling i utgangspunktet. Når en ny spørring blir mottatt blir denne informasjonen brukt til å avgjøre hvilken node som mest sannsynlig er kapabel til å hente de etterspurte data på minst mulig tid og den noden blir da spurt som et resultat av routing algoritmen.
En av de viktigste aspektene ved den nye routingen var å finne en måte å avgjøre hvor lang tid det ville ta å hente data gitt en hvilken som helst nøkkel etterspurt fra en hvilken som helst node. Det trengtes en respons tid estimator.
For å imøtekomme dette krevdes en algoritme som oppfyller disse kravene:

- Må ha muligheten til å gjøre utdannede gjetninger i forhold til nøkler som noden aldr før har sett
- Må være progressiv, slik at hvis en node forandre tilstand over tid skal dette bli presentert, men skal ikke være overfølsom for nylige fluks som kan avvike dramatisk fra gjennomsnittet
- Må være ”scale free”
- Må være effektivt serialiserbar

En enkel algoritme ble utviklet som møtte disse kriteriene. Den virker ved å opprettholde N referansepunkter (hvor N er konfigurerbar og 10 er en vanlig verdi) som er distribuert jevnt over nøkkelrommet (keyspace). Når det oppstår et nytt tids ”sample” på en gitt nøkkel, beveger vi de to punktene som liggere nærmest mot den. Hvor mye de beveger seg kan justeres for å bestemme hvor glemsk responstidsestimatoren skal være.



På diagrammet over kan vi se at de to referanser punktene (blått) beveger seg mot vår nye data “sample” (rød).
Når vi ønsker å lage et anslag for en ny nøkkel, ser vi på hvor linjen mellom de to referansepunktene skjærer (grønn), og dette gir tilnærmings vis responstid.

Behandling av forskjellige datalengder. Vi må ta med at det er annet aspekt ved å avgjøre tiden det tar å hente data. Ikke bare responstiden, men også trafikk tiden, den tiden det tar å sende de fysiske data. Det måtte utvikles en metode for å få rapportert en samlet verdi ut fra disse to tilbake til routingalgoritmen for å gi nøyaktige estimater. Dette gjøre ved å bruke et gjennomsnitt på datalenge i Freenet. Summen av disse to blir så brukt til å gi estimatet.

Behandling av mislykkede oppkoblinger. Med noder som er overbelastet er det mulig at vi ikke kan opprette tilkoblinger mot, og det kan redegjøres for denne muligheten ved å hente informasjon basert på et gjennomsnitt av mislykkede oppkoblinger og hvor lang tid dette tok. Så kan denne informasjonen leggest til i den estimerte routing tiden til den noden. Nedarvet kunnskap. Et av problemene ved Freenet i dag er den tiden som kreves for en node å opprette nok kunnskap om Freenet (andre noder) til å route effektivt. Dette problemet er åpenbart for nybegynnere på Freenet og oppleves som treghet. Løsningen på dette problemet er å implementer noe som gjør at noder kan stole på hverandre slik at de kan dele informasjon om hverandre. Det er to måter å gjøre dette på. Den første måten er å laste en ”seednode.ref” fil når noden startes som inneholder andre noders routing erfaringer, og da fra erfarne noder. Med den nye generasjon routing vil informasjonen i denne filen inneholde statistiske data slik at når en ny node starter opp og laster denne filen vil den i realiteten allerede være en erfaren node. Så vil denne node begynne å raffinere sin posisjon i nettverket og etter hvert kanskje spesialisere seg. Den andre måten noder lærer om nye noder er i datakilde feltet for vellykkede svar på spørringer. Datakildefeltet vil innholde en av ”upstream” nodene i den kjeden spørringen går gjennom. Den enkle fremgangsmåten ville være å tillate denne datakilde noden å hekte på statistisk informasjon som omhandler dens egen ytelse i svaret den returnerer, men dette ville selvsagt kunne missbrukes.

En litt mer raffinert metode vil være å tillate en hvilken som helst node som sender et svar oppover kjeden og som har samlet sin egen informasjon om noden i datakilden, å bytte ut den statistiske informasjonen med sin egen og legge denne ved i svaret. Dette betyr at uansett om en node sender misvisende informasjon tilbake opp kjeden, så vil denne antakeligvis bli overskrevet på sin ferd tilbake til den noden som sendte spørringen i utgangspunktet.

Fordelene ved neste generasjons routing.

- I den gamle Freenet algoritmen ble en node som satt bak et modem behandlet likt med en node som satt bak en bredbands tilkobling. Den underliggende internettopologien blir ignorert og alle noder blir behandlet likt. Neste generasjons routing baserer sin routing avgjørelser på faktiske routing tider. Dette betyr at en node vil helle mot å sende forespørsler til en raskere node, på raskere Internet oppkoblinger som ligger geografisk nærmere. Dette vil føre til et raskere Freenet.

- Med den gamle tilnærmelsen til Freenet routing var den eneste sikre måten å evaluere effektene på å prøve nettet. Nå, med den neste generasjon routing kan effektiviteten og forandringer i effektiviteten lett måles ved å se på forskjellen mellom forventede routingtider og faktiske routingtider. Hvis en forandring i algoritmen gir nærmere estimater, så vet man at forandringen har gjort algoritmen bedre

- Hvis en godtar at i et miljø hvor ens egen node er den eneste som kan stoles på er det rimelig fornuftig å anta at avgjørelser skal kun tas på bakgrunn av egne observasjoner. Gitt dette, så kan man si at hvis vi gjør bruk av tidligere observasjoner for å ta routing avgjørelser, kan vi si at vår routing algoritme er optimal. Det vil selvfølgelig alltid være rom for forbedringer, for eksempel der hvor algoritmene avgjør routing tider.

[8]

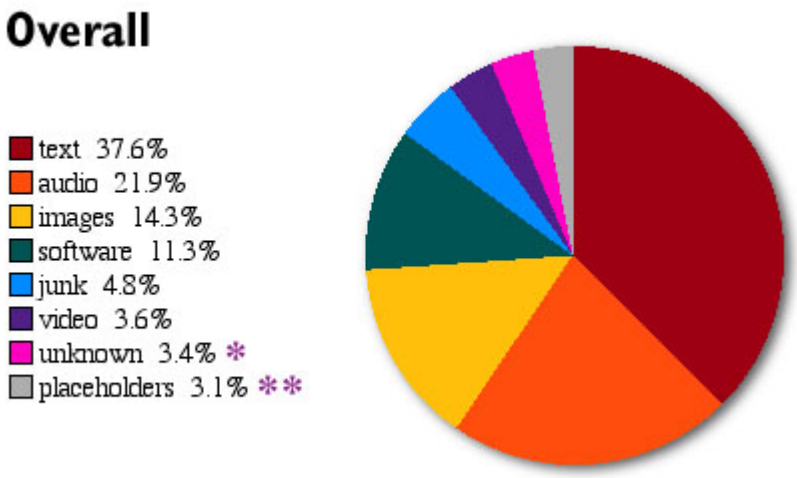
[8] http://Freenetproject.org/index.php?page=ngrouting

Statistikk

Det er mange problemstillinger som må tas stilling når man skal lage statistiske oversikter i forhold til Freenet. For det første må en tenke på Freenets arkitektur og routingsprotokoll, som gjør at du begår en straffbar handling i det du forsøker å røre ved filer på Freenet som i seg selv er ulovlig. Idet du åpner noe fra Freenet er du med på å spre innholdet. Videre tar slikt arbeid lang tid. Siden det ikke finnes noen iboende statistiske verktøy i Freenets arkitektur så må man sjekke alt innhold på Freenet på den vankelige og langvinte måten, nemlig ved å surfe på Freenet. Og i den sammenheng kan vi nok engang nevne at Freenet er fryktelig tregt, slik at det ikke er bare bare og skal surfe flere hundre eller gjerne flere tusen sider. Dette er noe vi ikke har hatt tid til, og med tanke på at vi sannsynligvis ville bryte en og annen lov i forsøket, så har vi "jukset" litt. Det vil si, vi har fått tillatelse til å bruke statistisk materiale samlet av Jon Orwant. Takk til Jon Orwant for dette.
Han har sjekket 1057 Freenetsider og deres innhold, og fra sine funn laget en oversikt som om ikke annet belyser fordelingen av materiale på Freenet. Vi vil poengtere at det er uvisst hvor mange Freenetsider det finnes der ute slik at dette resultatet kan være noe misvisende. I tillegg må det poengteres at denne undersøkelsen er basert på de offentlige sidene i Freenet. De sidene som ikke publiseres i Freenets offentlighet, slik som portalen The Freedom Engine er ikke tatt med, og kan heller ikke tas med av opplagte årsaker. Uansett så vil vi ha med denne oversikten, som muligens er den eneste som er utført, for å gi et lite innblikk i hva som befinner seg der ute.

Det første diagrammet viser totalen basert på alle sidene som ble undersøkt, deretter følger diagrammer til alle delene av hoveddiagrammet med korte forklaringer i forhold til funnene.

Totalt

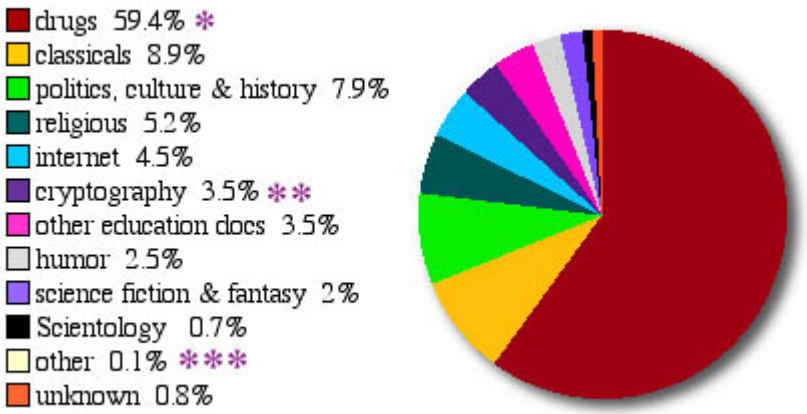


* Ukjent men ser meningsfylt ut
**Indekser til annet Freenet innhold

Diagrammet over gir oss opplysninger om at tekst(37,6 %), lyd(21,9 %) og bildefiler(14,3 %) er godt representert i Freenets innhold. Det må også sies at for eksempel Ruth Rendel lyd bok (som var ble betegnet som lydfil) var oppdelt i fire filer. Mange av nøklene hadde også ulike navn men likt innehold. Som for eksempel: *docs/books/english/fiction/george_orwell/1984.htm* og *docs/books/english/fiction/george_orwell/1984.htm.zip*

Tekst

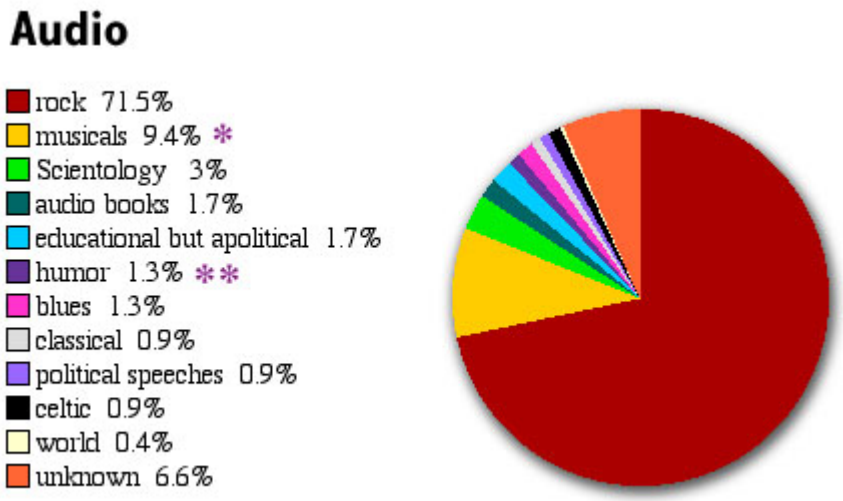
19.1 % så ut til å være bøker og 80.9 % var vanlige dokumenter, selv det ofte var vanskelig å skille mellom de to



* De fleste forbudt i USA
** Inkludert dokumenter om Freenet
*** Bøker som er beskyttet av kopirettigheter

Det var en' O'Reilly bok blant alt dette; The PDF of Open Sources. Dette var også den eneste boken om datamaskiner. En Harry Potter novelle og George Orwell's 1984 var også å finne.

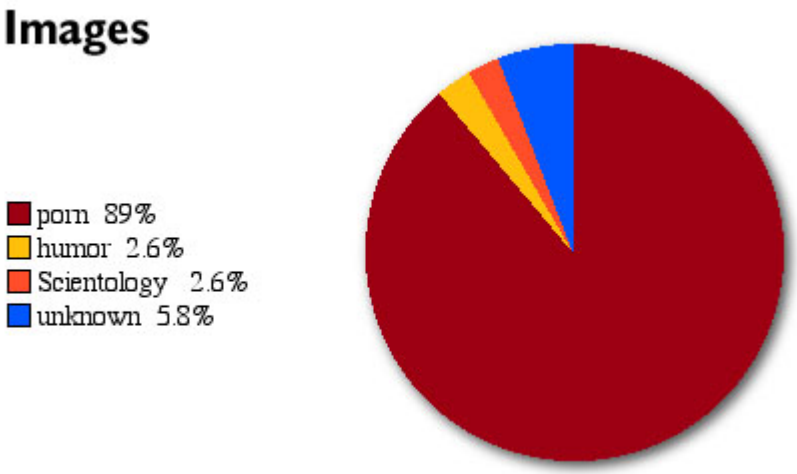
Lyd



* Alle var "Jesus Christ Superstar"
** Tom Lehrer, weird Al Yankovic og Monty Python

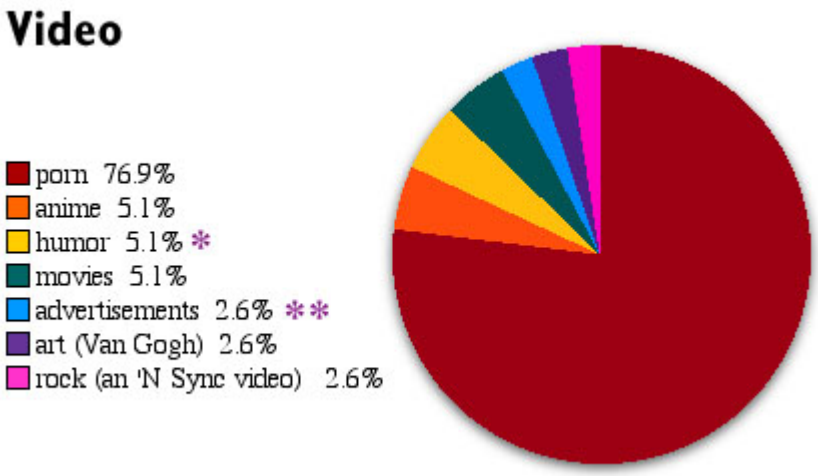
Det finnes hele album av noen band som Genesis, Eurythmics, Alphaville, Stereolab, Information Society og Sinead O'Connor. Vi tar med at selv om musikken som er å finne på Freenet stort sett er av typen rock, så vil slike statistikker basert på nøkler i Freenet overrapportere rock i forhold til klassisk siden et rockealbum ofte inneholder langt flere låter enn et klassisk album.

Bilder



Blant pornobildene var det fire med navn som tilsa at det var overgrepsbilder. Det må legges til at bildene er kategorisert etter navnene til nøklene som peker til bildene. Jeg har ikke sett noen av bildene.

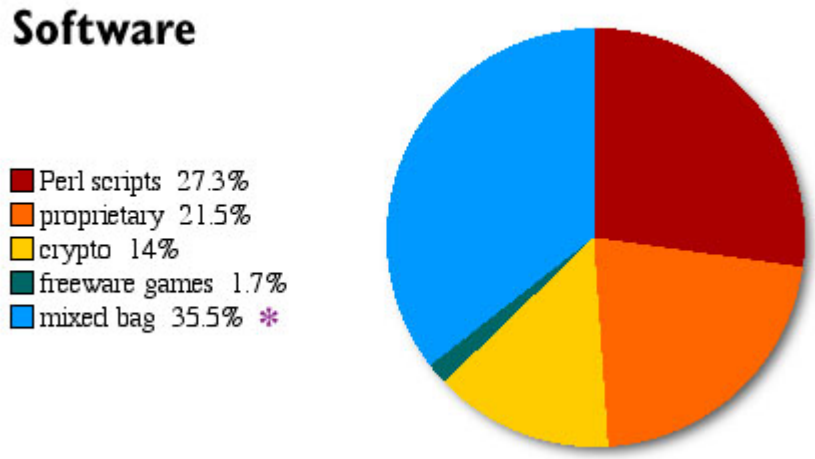
Video



* Dilbert Shockwave animasjoner
** En Arnold Schwarzenegger reklame

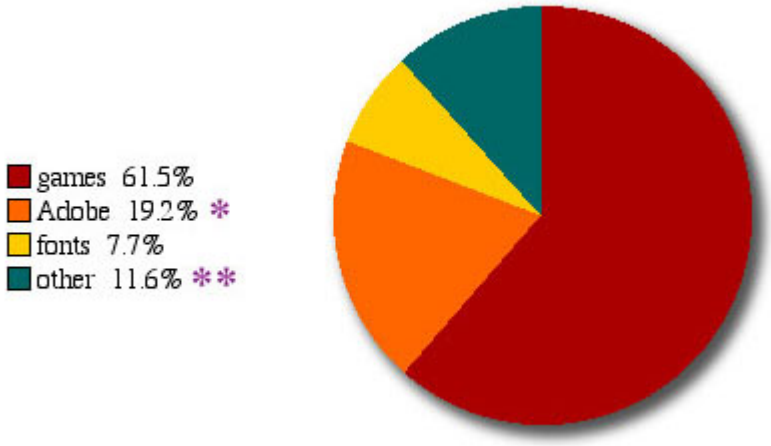
De to spillefilmene som ble funnet var Matrix og Scary Movie

Programvare



* Inkluderer to C programmer og ingen annen klart identifiserbar kildekode

Av beskyttet programvare:



* Programvarepakker
** Inkluderer Mathematica

Av de kopibeskyttede spillene var 81,2 % av dem til Nintendo konsoller

Media på Freenet i forhold til statistikken

Porno: 15,6%
Sex, drugs and rock'n'roll: 53,8%

Hvis vi skal lage en demografisk beskrivelse av den gjennomsnittlige Freenet bruker ut fra denne statistikken så ville han eller hun være en Crypto-anarkistisk Pearl Hacker, med sans for klassisk litteratur, politiske "screeds", 80-talls pop musikk, Adobe programvare og mye porno.[9]

[9] http://www.openp2p.com/pub/a/p2p/2000/11/21/Freenetcontent.html
gjelder alt statistisk materiale under kapittelet; Statistikk

Konklusjon

Vi vil her benytte anledningen til å si at arbeidet med utformingen av denne rapporten har ført oss inn i de mørkeste korridorer i menneskesinnet, og har blottlagt en skjult verden vi aldri kunne ha forestilt oss. En verden hvor voksne mennesker ødelegger barn for profitt eller seksuell tilfredsstillelse. Vi sitter igjen med tårer i øynene og en bitter smak i munnen. Når det er sagt kan vi legge til at flere mennesker burde opplyses om de faktiske forhold. Denne krigen trenger flere soldater hvis vi skal ha noen som helst sjanse til å vinne.

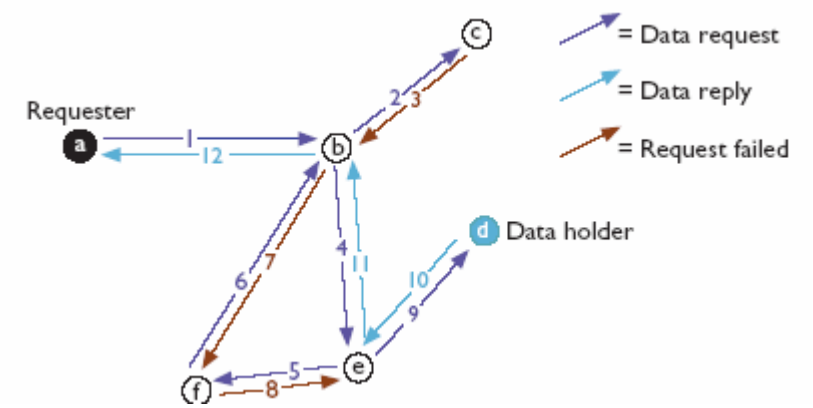
Hvis man skal ha noen som helst mulighet til å gjøre noe med utviklingen i forhold til produksjon, distribusjon og bruk av overgrepsbilder trenger regjeringene i alle land å våkne. Det kreves mer penger og flere folk til å jobbe med denne problematikken.
Når det kommer til Freenet og spredningen av overgrepsbilder er det dessverre fryktelig lite man kan gjøre, så langt vi kan se. Nå skal det her tas med at vi som har utformet denne rapporten er studenter og ikke vet alt som er verdt å vite, men så langt som vi har forsket på Freenet kan vi konstantere at det er et ideelt sted for spredning av overgrepsmateriale. Nå vil vi også legge til at Freenet ikke er unikt i det henseende. Det finnes flere slike nettverk som bygger på den samme filosofien og teknologien. Men det er ikke tvil om at Freenet og deres skapere må ta en del av ansvaret for overgrepene som blir utført, dokumentert og publisert. Dette kan virke som en urettferdig og bastant påstand, men alt og alle som nører under og fostrer spredning, etterspørsel av slikt materiale og tilrettelegger for distribusjon er etter vår mening medansvarlige. Bilprodusentene blir ikke holdt ansvarlige når folk kjører seg i hjel, men er opp gjennom årene blitt pålagt av myndighetene å gjøre bilene de selger sikrere. Det er egentlig ingen grunn til at ikke dette også skulle gjelde tjenester som Freenet.

Vi er enige med tanken bak Freenet, med tanke på at det ikke er alle som får sagt det som trengs å bli sagt ute i verden, men når en ser på innholdet på Freenet så kan en jo stille seg spørsmålet om Freenet gjør mer skade enn gagn. Og det slår oss at hvis du lever i et land hvor du er undertrykt, har du da tilgang til pc, til Internet, og dermed Freenet? I de fleste tilfeller vil nok svaret være nei. Så om Freenet tjener sin ideologiske hensikt er heller tvilsomt. At det tjener de som driver med lyssky aktiviteter som distribusjon av overgrepsbilder er helt klart. Og dette rammer de aller svakeste i samfunnet på en verst tenkelig måte. Barna får livene sine ødelagt, opplever smerte, frykt, angst og ensomhet som resultat av dette, alle de ting de fleste av oss desperat forsøker å skjerme våre barn fra.

Ytringsfrihet og null sensur er vell og bra for å forme drivverdige demokratier som gjør livet til de aller fleste mennesker bedre, men til hvilken pris. Er det ikke enkelte ting som burde sensureres, som burde jaktes på og fjernes fra våre samfunn. Barna er vår fremtid, vår arv, og vi burde skamme oss for at vi ikke beskytter dem godt nok! Freenet er brikke i spillet om dokumenterte seksuelle overgrep mot barn, derom hersker ingen tvil, og det bør gjøres noe med dette så raskt som mulig.

FREENET

Beskrivelse av FREENET-konseptet med analyse og rapport.



Obligatorisk oppgave i IN116

Prosjektet er gjennomført vårsemesteret 2005 av:

Steinar Kulstad. steinar.kulstad@monet.no
Arnt Håvard Pettersen. arntpe@c2i.net
Felicia Dziales. feliciad@start.no
Svein Erik Molberg. svein.e.molberg@monet.no

1.år IT-Bachelor.
Høgskolen i Nesna

Versjon. 2.1
30.03.2005

Innledning

Freenet er et slags "Internett i Internett", der all forbindelse er kryptert.
NyeKRIPOS er urolig for hva som kan skje dersom distributører og overgripere flytter produksjonen av overgrepsbilder av barn ut på dette nettet.
Både HiNe og NyeKRIPOS vil gjerne ha en analyse av Freenet-konseptet og på hvilken måte dette nettet kan vanskeliggjøre etterforsking av seksuelle overgrep mot barn og bilder/ film som dokumenterer disse overgrepene, og om det eventuelt finnes muligheter å spore ulovlig aktivitet også her.
Brukes det til distribusjon av overgrepsbilder i dag? Er det mulig å finne ut av det?

Freenet var ukjent for gruppa da vi startet opp med oppgaven, men vi hadde litt kjennskap til andre fildelingsnettverk. Vi samlet inn materiale og teknisk dokumentasjon for å sette oss inn i hva Freenet egentlig er. Vi satte opp to datamaskiner for oppkobling og installering av Freenet. Det ble laget en del tekstfiler som ble distribuert på Freenet for å teste hvordan Freenet fungerer. Etter hvert har vi fordelt oppgavene for kunne fordype oss i de enkelte områdene for nærmere studier av Freenet.

Oppgaven har vært veldig interessant og utfordrende, ikke minst med tanken på å kanskje kunne hjelpe NyeKRIPOS i kampen mot seksuelle overgrep mot barn og spredning av overgrepsbilder.

Historie.

Historien om Freenet.

Freenet er et Internett i Internett som er laget for anonym informasjon og filutveksling.
Freenet er en gratis programvare som er laget for å sikre fri kommunikasjon over Internett. Programmet tillater alle å publisere og lese informasjon med full anonymitet.
Med Freenet knyttes et dataobjekt til en nøkkel, og dersom du søker med denne nøkkelen kommer selve dataen til maskinen din.
Freenet versjon 0.1 ble registrert første gang 28.12.1999, i dag foreligger Freenet versjon 0.5.[10]

Grunnlegger:
Ian Clark er grunnlegger og har hovedideen bak Freenet., han er født i Dublin, Irland den 16 februar 1977. Han studerte informatikk ved Universitetet i Edinburgh. Som avslutning på studiet skrev han hovedoppgaven ”A Distibuted Decentralised Information Storage and Retrieval System”. Det var denne rapporten som ga grunnlag for Freenet. Han ville lage et system som skulle være 100% motstandsdyktig mot sensur, dette for å verne om ytringsfriheten. Som han selv sier til Wired News: ” Hvis du tror på ytringsfrihet må du også beskytte andre menneskers rett til det samme... selv når du er uenig eller synes ytringsfrihet er usmakelig. Freenet er som en parallell Word Wide Web hvor alle er anonyme”. I et annet intervju til O´Reilly på websiden openp2p.com sier Clark: ”Ideen var todelt, først filosofien, frihet til å kunne si og publisere hva en vil uten sensur. Jeg er bekymret for begrensingene på dette i Internett. Regjeringene i Vesten har sine lover om hva en kan si og gjøre på Internett, og hvordan ting skal utføres, også i henhold til betaling og priser. Tenkte også på menneskene i Kina og Saudi-Arabia der det er enda større sensur enn i Vesten. At de kan få muligheten til å utveksle informasjon mer sikkert.
Det andre trekkplasteret bak Freenet er det tekniske. Dagens WWW utnytter ressurser dårlige. Hvis 1000 mennesker i f.eks. UK (Unitet Kingdom) laster ned det samme dokumentet må det reise 1000 ganger over Atlanteren før det kommer fram, med Freenet reiser det bare 1 gang over samme strekning før det lagres i nærheten”.

[10] http://www..sv.uio/mutr/publikasjoner/rapp2003/rapport53/index-Freenet.html

Realisering:
Ian Clark innledet samarbeid med en rekke utviklere fra forskjellige land for å utvikle teknologien og ideene som var kommet fram i hovedoppgaven fra universitetet. De laget ett system hvor dokumenter kan publiseres og leses fritt uten at de kan spores til en bestemt fysisk eller geografisk nettadresse, et nettverk av dokumenttjenere som kjøres på internettmaskiner. Dokumentene og deres plassering ble beskyttet med sterk kryptering.
De andre utviklerne er: Oskar Sandberg, Brandon Willy og Theoore W. Hong.[11]

[11] http://www.openp2p.com/pub/a/p2p/2000/11/14/ian.html

Definisjoner og begreper.

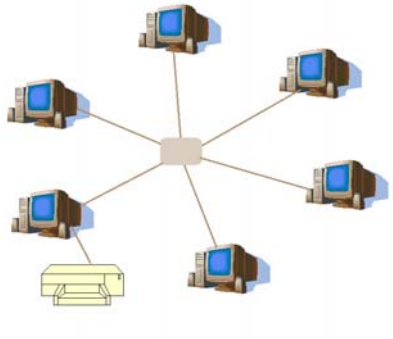
For å forstå hva Freenet er må en del begreper og definisjoner klarlegges. Begreper som kommer til å gå igjen er ” noder, P2P, nøkler, krypteringer ” osv. Vi skal her prøve å gjøre rede for disse begrepene på en forståelig måte.

Hva er så node til node og P2P?

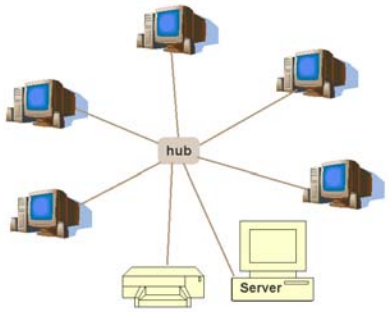
NODER: Felles betegnelse for alle enheter som er koblet til et netverk.

Peer-to-Peer (P2P): Et nettverk der klient-pc-er kommuniserer direkte med hverandre uten en dedikert tjener. Hver enkelt klient-maskin i et P2P-nettverk fungerer nemlig som både klient og tjener. En annen måte å definere P2P på er som "et desentralisert, selvorganiserende, distribuert system".

Peer to Peer nettverk:



Klient - Tjener nettverk:

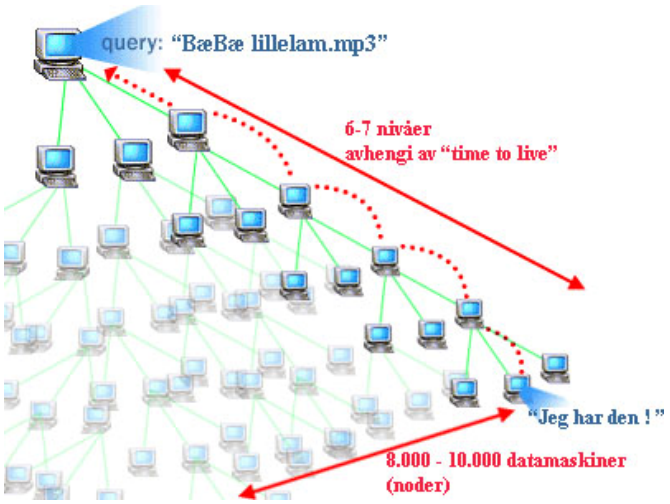


Node-til-node-teknologi (peer-to-peer – P2P) ble første gang allment distribuert og populær i fildelingsprogrammer som Napster og KaZaA. I denne sammenhengen kan node-til-node-teknologien brukes til å dele, søke etter og laste ned filer.

Etter vår oppfatning betegnes et ekte node-til-node-system av at alle nodene i et nettverk kobles sammen dynamisk, for å delta i oppgaver som omfatter ruting av trafikk, prosessering og båndbreddehåndtering, noe som ellers vanligvis håndteres av sentrale servere.

FastTrack (node-til-node-teknologien bak KaZaA) var det første virkelig desentraliserte node-til-node-programmet, og det var banebrytende for SuperNoder-konseptet. Denne tilnærmingen er senere tatt i bruk av mange fildelingsteknologier, blant annet senere versjoner av Gnutella.

Eksempel på en spørring i et P2P nett:



Desentraliserte node-til-node-nettverk, som FastTrack, har mange fordeler fremfor tradisjonelle klient-server-nettverk. Disse nettverkene kan bli uendelig store, uten redusert søketid og uten behov for kostbare, sentraliserte ressurser. De bruker prosessor- og nettverkskraften i sluttbrukermaskinene fordi disse ressursene alltid øker direkte proporsjonalt med nettverket. Hver nye node som legges til i nettverket, legger til potensiell prosessorkraft og båndbredde i nettverket. Ved å desentralisere ressursene, har andre generasjons (2G) node-til-node-nettverk gjort det mulig å praktisk talt fjerne kostnader forbundet med en stor sentralisert infrastruktur.

Tredje generasjon P2P representert av eDonkey og nå Morpheus og en del mindre uavhengige utviklere, gjør verktøyene mer desentralisert enn noen sinne. Neonet -teknologien er rett og slett en måte å ta et "snapshot" av lokasjonen til hvor hver eneste fil på nettverket befinner seg i et gitt øyeblikk og sprer biter av den informasjonen over hele nettverket.

For å finne en fil, går henvendelsen først til hvilken som helst datamaskin på nettverket. Den datamaskinen vil peke til en annen som har mer informasjon om hvordan filen skal finnes. Den tredje datamaskinen kan ha informasjon om selve filen eller den kan ta et par hopp for å finne datamaskinen med rett informasjon.

Prosessen fungerer litt som å spørre mer og mer informerte turistguider etter veien. Som sammenliknet med forrige versjon var å spørre tilfeldige personer på gata. Informasjonen om nettverket blir konstant oppdatert etter hvert som nye filer og datamaskiner dukker opp.

Begrepsavklaring

- **Kryptering:** Dataen blir endret til meningsløse data foruten de som har nøkkelen som må brukes for å dekryptere (tilbakestille) dataene.
- **Web interface brukergrensesnitt:** Programmet åpnes fra en nettleser slik som Explorer. Opera eller Firefox.
- **Freeware:** Gratis programvare.
- **Frost:** En fildelingsklient med et grafisk grensesnitt som brukes mot Freenet. Ikke ulik de kjente fildelingsprogrammene Kazaa og Gnutella.
- **Localhost:** IP adresse 127.0.0.1 Det er den lokale adressen til maskinen (ikke ut i verden)
- **Server:** En maskin som er koblet til nettet og som brukere kan koble seg opp mot. En webserver leverer websider, en filserver inneholder filer som brukerne kan laste ned.
- **Anarkisme: ~is'me** -*n* politisk bevegelse som vil erstatte staten og alle styrende organer med frivillig samarbeid av individer og grupper
- **Anarki: anarki'** n3 (fra gresk, av *anarkhos* 'uten leder, fører') samfunnstilstand uten lover og statsmakter; lovløshet *borgerkrig med a- / det råder det rene a- i skoletimene*[12]
- **Gateway:** En gateway er en maskin og/eller programvare som kobler sammen nettverket slik at data kan overføres mellom dem. Brukes synonymt med ruter da en gateway er IP-adressen til en ruter.[13]
- **Seednode.ref:** En referansefil som gir brukeren en nøkkel til nettverket, det følger med en standard referansefil kalt Seednode.ref men det kan brukes andre brukeres referansefiler.
- **Datastore:** Den delen av harddisken som man setter av på maskinen som nettverket har til rådighet for å lagre filene som publiseres og motas.
- **URI:** Uniform resource identifier En fil's adresse identifikasjon på internett.
- **Kryptografisk hashing**: Kryptografiske teknikker benyttes til alle former for beskyttelse av data, som sendes, f.eks. over Internettet. Typisk bruk for at datainnholdet ikke skal kunne endres uten at det vil bli avslørt. Hvilket gjøres med en spesiell teknikk som kalles hashing, et slags fingeravtrykk. Denne hashverdien låses ved hjelp av en eller annen form for nøkkel.[14]
- **Ondsinnede noder:** Enhet som forsøker å ødelegge eller spre feilinformasjon, virus eller på annen måte skade nettverket.
- **Nøkler:** Er krypterte adresser, dokumentnavn og eierrettigheter.

---

[12] http://www.dokpro.uio.no/perl/ordboksoek/ordbok.cgi?OPP=anarki&bokmaal=S%F8k+i+Bokm%E5lsordboka&ordbok=bokmaal&alfabet=n&renset=j

[13] http://itpro.no/art/5900_printable.html

[14] https://www.cert.dk/artikler/artikler/000999A028.shtml

Nøkler i Freenet.

En sentral del av Freenet består av såkalte nøkler. Disse nøklene har forskjellige egenskaper og bruksområder. Vi skal her forsøke å redegjøre for disse nøklene.

Brukernøkler.

Brukernøklene benyttes av Freenet-brukeren. Disse konverteres videre til søkenøkler og krypteringsnøkler. Får hente et dokument i Freenet benyttes nøkler kalt URI (Unique Resource Identificator), de kan sammenlignes med en URL adresse i internett, som også er en slags nøkkel som brukes til å hente et dokument. Nøklene har ingen betydning for nodene, men brukes av klienten til å fortelle den lokale noden hva den skal gjøre.
Brukernøklene benyttes til å tjene Freenets hensikt. La oss tenke oss at Freenet er et området hvor alle kan hente data, lagre data, publisere hva de vil og den informasjonen som blir publisert skal være tilgjengelig for alle som er tilkoblet. Da må man i praksis ha retningslinjer for hvordan den enkeltes tilgang kontrolleres.
Siden området består av mange sammenkoblede noder, kan man i utgangspunktet ikke vite hvilke noder som tjener nettes hensikt, og hvilke som forsøker å undergrave det. Nettet må derfor beskyttes mot angrep som kan undergrave den informasjonen som er lagt inn, og også beskytte brukernes egentlige identitet.

Dette kan oppsummeres gjennom følgende retningslinjer:

- Alle skal kunne hente ut dokumenter i Freenet, gitt at de har dokumentets URI (brukernøkkel).
- Alle skal kunne legge inn dokumenter.
- Lagringsplassen skal aldri ta slutt. Det betyr at dokumenter som forespørs sjelden må vike plass for de som forspørs ofte.
- Dokumenter som legges ut skal ikke kunne endres av andre enn forfatteren.
- Forfatteren skal ikke behøve å avsløre sin identitet.
- All datatrafikk skal kunne verifiseres av alle nodene trafikken går gjennom, slik at en kan sikre at noder ikke sender ut feil data.
- Brukere skal ikke enkelt kunne finne ut hvor dokumenter er fysisk lagret.

Alle disse retningslinjene tilfredsstilles ved hjelp av brukernøklene.

Dokumenter i Freenet lagres sammen med en søkenøkkel som identifiserer dokumentet. Søkenøklene er interne primitive nøkler, og en vanlig bruker kommer derfor ikke i direkte kontakt med disse. Brukeren benytter seg av nøkler som er leselige, som er brukernøkler (URI). Brukernøklene gjøres om til en søkenøkkel gjennom et eller flere ledd i brukerens Freenet klient, for deretter å sendes ut på den lokale noden, som ruter forespørselen videre.

Alle dokumenter blir kryptert før de sendes ut, ved hjelp av en symmetrisk chiffer. En klient må derfor vite hvilken nøkkel som ble brukt til å kryptere dokumentet, for å kunne dekryptere det. Dokumenter som legges ut på Freenet krypteres ved hjelp av en krypteringsnøkkel. Krypteringsnøkkelen blir ikke sendt sammen med forespørselen etter et dokument, men genereres i Freenet klienten. Når det forespurte dokumentet kommer til klienten, blir innholdet dekryptert ved hjelp av krypteringsnøkkelen og blir lagret der hvor brukeren har bestemt hvor det skal lagres.[15]

Søkenøkler.

Søkenøklene blir laget av Freenet-klienten basert på hvilken brukernøkkel som er blitt gitt av brukeren. Disse nøklene kan sammenlignes med IP-adresser på Internet. På samme måte som en Internet-URL blir konvertert til en IP-adresse av en DNS-server, blir brukernøklene konvertert til søkenøkler av Freenet-klienten. Hvordan konverteringen skal foregå er lik i alle klienter, slik at en brukernøkkel (URI) alltid konverteres til den samme søkenøkkelen. Søkenøklene brukes av nodene til å finne hvilken node som inneholder et dokument, og følger derfor en forespørsel gjennom hele dens levetid fra node til node. Alle dokumenter må derfor ha hver sin unike søkenøkkel for at det ikke skal oppstå kollisjoner.[16]

[15] Jonny Egeland, al, Semesteroppgave i TE6013 (2001) s.9 og 11

[16] http://216.239.59.104/search?q=cache:c4Ds_RgcrGkJ:www.ux.his.no/~sfm/Datasikkerhet2001/Semesteroppgaver2001/Freenet/Freenetrapport.doc+%E2%80%A2+Symmetriske+Blokkchiffre&hl=no

Krypteringsnøkler.

Krypteringsnøkler er nøklene som brukes i kryptografisk sammenheng i Freenet. All informasjon som publiseres på Freenet er kryptert, slik at de som kjører en node på sin egen maskin ikke skal kunne vite innholdet i dokumentene som lagres på sin egen maskin. Det er også ønskelig at innholdet pakkene som sendes er korrekte i forhold til det som ble forespurt, slik at ondsinnede noder kan detekteres og stenges ute. Det benyttes 3 grunnleggende teknikker innenfor kryptografi i Freenet.

- Kryptografisk hashing: Benyttes i alle tilfeller der en skal finne en hash til noe. Brukes til blant annet å generere søkenøkler og til verifisering av innhold.
- Symmetriske Blokkchiffre: Brukes til kryptering av dokumenter før de legges ut på nettet og kryptering av trafikken mellom noder.
- Public Key algoritmer: Benyttes til digital signering av dokumenter og nøkkelutveksling. Signering har tre formål: Vite at to dokumenter signert med samme signatur, har samme kilde(opphav). Signaturen settes ikke i sammenheng med identitet (holder signaturens eier anonym). Gir eier av dokumentet tillatelse til å endre innholdet i egne dokumenter.

Nøkkelutvekslingen brukes i kommunikasjon nodene i mellom og gjør det mulig å kryptere pakkene som sendes fra node til node. Dette gjør at forespørslene vanskelig kan identifiseres av utenforstående. Og selve innholdet er kryptert med symmetriske blokkchiffre.

Om Freenet.

Litt om programmet!

For tiden er det denne versjonen som ligger ute på download.com[17]: **Freenet 0.5.2.8.**

Programmet som først innstalleres er på 125.2kb og krever Windows 95/98/Me/NT/2000/XP, Java Virtual Machine. Selve programmet som lastes er på 11598kb. Det er en avinnstalleringsfunksjon inkludert i programmet, og programmet er det vi kaller freeware.
Til dags dato er det bare fra download.com lastet ned 59 291 kopier av programmet.

For å komme i gang med å bruke Freenet, trenger man en nodereferansefil kalt ”seednodes.ref”, som man kan motta fra en venn eller man kan koble til en server (Free Net Prosject server) for å motta filen. Programmet har et web-brukergrensesnitt ala phpmyadmin.

Freenet er et nett i Internett. Freenet er *ikke* world-wide-web. Freenet ligner på et fildelingsnettverk (P2P), men med en helt annen intensjon og virkemåte. Om Freenet er et fritt og demokratisk nett eller et fristed for de ekstreme er opp til deg å bestemme.[18]
Filene/websidene i Freenet ligger ikke på et bestemt ”fysisk” sted. (webservere, filservere) Nettverket sprer informasjonen på nodene etter hvor populær den er. Dette innebærer at en populær side eller fil vil ligge på mange steder/noder i Freenet, mens informasjon som ingen etterspør vil ”dø ut”. Informasjonen lagres i en ”datastore” hos den enkelte bruker. Brukeren selv vil ikke kunne se hva som er lagret i sin egen ”datastore” (informasjonen er tungt kryptert med 128-, 192-, eller 256-bit nøkler). Fra bla annet Twofish:

Twofish is a block cipher by Counterpane Labs. It was one of the five Advanced Encryption Standard (AES) finalists. Twofish is unpatented, and the source code is uncopyrighted and license-free; it is free for all uses.[19]

Brukeren kan riktignok selv velge størrelsen på sin egen ”datastore”.
Den enkelte bruker av Freenet har/er en egen node. Noden sender og mottar informasjon fra andre kjente noder i nettverket. All trafikk i nettverket er kryptert, både forespørsel og nedlasting.

[17] http://www.download.com/3001-2196_4-10214417.html
[18] http://itpro.no/art/725.html
[19] http://www.schneier.com/twofish.html

Hvordan distribuere filer/ finne informasjon / på Freenet?

Informasjonen sendes ut i Freenet (filer eller nett-sider) av den enkelte bruker. Det er umulig å vite hvor den havner; din egen ”datastore”, naboens eller ett eller annet sted i verden.
Så snart du har Freenet i gang kan du åpne en ”gateway” i din vanlige nettleser.(localhost) Her finner du noen linker til nettsider i Freenet, og disse siden kan brukeren selv redigere slik at gatewayen blir som en en personlig portal til sider som brukeren liker/besøker ofte. Når det gjelder søking etter filer er det utviklet flere klienter med samme grensesnittet som vanlige p2p fildelingsprogram, FROST er en slik klient.

Hvordan komme seg på Freenet?

Gå til siden Download Freenet for å komme i gang. Det kan være problemer med å få tak i riktige referansefiler (seednode.ref), da de som følger med i innstallasjonen ikke alltid fungerer. Foreløpig er det litt for vanskelig for den ”vanlige” PC-bruker å komme seg på Freenet dersom det ikke fungerer med en gang, men dette forventes å bedres etter hvert som prosjektet utvikles.

Positive sider ved Freenet:

- Anonymitet for den enkelte bruker
- Ingen sensur – fremmer ytringsfriheten
- Er/kan bli et verktøy for mennesker i land uten fri meningsflyt (Kina, Nord Korea, Burma etc.)

Negative sider ved Freenet:

- Tregt (grunnet tung kryptering og det at prosjektet vil være under utvikling i en god stund fremover)
- Høy ”brukerterskel” (foreløpig vanskelig)
- Foreløpig ikke søkemuligheter slik man er kjent med i www (Frost er en klient ala Kazaa)
- Også nazister, terrorister og pedofile vil kunne bruke/bruker i aller høyeste grad Freenet
- Den enkelte bruker har ingen kontroll over hva som lagres på egen maskin (”datastore”) da alt er kryptert. [20]

[20] http://itpro.no/art/725.html

Anonymitet

Tanken bak Freenet.

For å oppnå frihet fra kontroll er nettverket helt desentralisert og utgivere og brukere av informasjonen anonyme. Uten anonymitet er man ikke sikret full ytringsfrihet uten represalier i regimer som f.eks Burma, Kina og Nord Korea. Og uten desentralisering vil nettverket lett bli utsatt for angrep ved at servere blir beslaglagt av det enkelte lands myndighet.
Kommunikasjon gjennom Freenet noder er kryptert og "dirigert" gjennom andre noder for å gjøre det ekstra vanskelig å fastsette hvem som ber om informasjonen og hva innholdet er.
Brukere bidrar til nettverket med båndbredde og harddisk-plass (kalt "the data store") for å lagre filer. Freenet, i motsetning til andre felles nettverk, lar ikke brukeren kontrollere hva som blir lagret i "the data store". I stedet blir filer beholdt eller slettet avhengig av hvor populære de er. Upopulære filer blir slettet for å gi plass til mer populære filer. Filer i " the data store" er kryptert slik at sannsynligheten for å bli saksøkt av personer som ønsker å sensurere innhold i Freenet reduseres.
Nettverket kan brukes på en rekke forskjellige måter og er ikke begrenset til bytting av filer mellom kamerater. Det fungerer heller som et Internett i Internettet.

Freenet kan for eksempel bli brukt til:

- Publisere nettsider eller "Freenet" sider
- Kommunikasjon gjennom (meldingstavler?)
- Innholdsdistribusjon

I motsetning til mange banebrytende prosjekter har Freenet for lengst forlatt forsøksrommet. Det har blitt lastet ned av over to millioner brukere siden prosjektet startet og blir brukt i distribusjon av sensurert infomasjon over hele verden, inkludert Kina og Midtøsten. Ideer og konsepter først utarbeidet i Freenet har hatt en betydelig innvirkning på den akademiske verden. ”Vår nettavis "Freenet: A Distributed Anonimous Information Storage and Retrieval System" var den mest besøkte ITK avisen i år 2000”, i følge "Citeseer". Freenet har også inspirert aviser innen jus og filosofi. Freenets skaper og prosjektcoordinator, Ian Clarke, ble utpekt til en av de 100 beste innovatorer i 2003 av MITs Technology Review magazine.[21]

[21] http://Freenet.sourceforge.net/index.php?page=whatis

Hvorfor anonymitet?

Anonymiteten i ”Peer to Peer” nettverket Freenet er svært godt sikret. Det er vanskelig å spore hvilken informasjon man henter fra nettet og hvem som har lagt ut informasjonen. Som utgiver av informasjonen kan man skjule sin egentlige identitet enten ved at man benytter en falsk eller ingen identitet. Tanken bak Freenet var å lage et medium med total ytringsfrihet. For å få dette til mente man at det var nødvendig forhindre at noen kunne kontrollere informasjonsflyten. Som betyr at dersom ingen har kontroll over hvilken informasjon som blir gjort tilgjengelig kan det heller ikke bli gjennomført sensur. Det ble også sett på som nødvendig å gi mulighet for total anonymitet i et slikt nettverk fordi det er mye lettere å straffe folk for å benytte seg av ytringsfrihet enn å hindre dem i å gjøre det. Frykten for en slik straff kan også hindre folk i å publisere sine meninger. Et annet viktig punkt er lagringen av informasjon på Freenet. Dersom det er mulig å spore opp hvor informasjon er lagret muliggjør dette sensurering av uønsket materiale ved angrep på disse serverne. I det Freenet som eksisterer i dag er det gjort vesentlig vanskeligere å spore både sender, mottaker og den som lagrer informasjon enn i Internettet som sådan.[22]

Sikkerhet i Freenet.

Som tidligere nevnt legges det stor vekt på anonymitet og sikkerhet i Freenet. Derfor er all informasjon og kommunikasjon på Freenet kryptert og digitalt signert slik at en ikke kan forandre på dataene som er lagt ut eller blir sendt. Freenet skiller seg særlig ut i fra de andre peer to peer nettverkene med at det skal være tilnærmet umulig å fjerne informasjon som er publisert. Når en legger ut informasjon på Freenet har en ingen mulighet til å bestemme hvor denne informasjonen skal lagres. Det er bare utgiveren som har muligheten til å forandre på den informasjonen han har lagt ut, ved at han har en privat nøkkel i tillegg til den offentlige nøkkelen. Prøver noen å slette et dokument skaper det redundans og dokumentet kopierer seg selv og i tillegg kan dokumentet ligge på andre noder langt unna. Hvis et dokument ikke blir forspurt vil det ”dø ut” av seg selv etter en tid. Dette på grunn av at de mest etterspurte dokumentene hele tiden vil ha prioritet fremfor de minst etterspurte dokumentene og vil presse ut de gamle. Dette gjør at det er vanskelig å vite hvor og hvor mange plasser informasjonen lagres.[23]

[22] Jonny Egeland, al, Semesteroppgave i TE6013 (2001) s.5 og 23.
[23] Jonny Egeland, al, Semesteroppgave i TE6013 (2001) s.5.

Sikkerheten til nodens eier.

En av primærhensiktene til Freenet å beskytte anonymiteten til de som legger ut data og de som mottar data. Sikkerheten for dem som lagrer informasjon i Freenet kan sees på fra to sider. For det første er det viktig at informasjonen som er lagret på noden er sikker mot angrep av personer som prøver å fjerne data fra nettet. Dersom noe er publisert på Freenet og det blir etterspurt er det viktig at det er vanskelig å få fjernet dette. Dersom man kan bestemme hvor noe er lagret gjør dette det mulig å utøve sensur på nettet ved å hindre de aktuelle nodene i å spre informasjonen. Dersom dette er umulig er det også umulig å fjerne denne informasjonen. En annen side av saken er sikkerheten for personene som eier nodene. Dersom det er mulig å bestemme hva en node lagrer er det også mulig å straffe eierne av noder som inneholder uønsket informasjon. Dette utgjør en stor trussel mot ytringsfriheten generelt på Internett, og er derfor også en viktig del av sikkerheten i Freenet. Begge disse problemene finnes det altså en viss beskyttelse mot i Freenet.[24]

En viktig detalj er å kunne hemmeligholde noder som lagrer informasjon slik at informasjonen ikke kan slettes. Dersom man etterspør en fil på Freenet vil etterspørselen bli routet via flere noder til filen blir funnet og så sendt samme ruten tilbake til mottaker. På hver av nodene som ligger mellom sender og mottaker vil filen mellomlagres og man kan dermed identifisere en node som lagrer denne filen. Den noden som til slutt sendte filen til mottaker må nødvendigvis lagre filen. Dette hjelper imidlertid ikke den som prøver å fjerne informasjon fra Freenet. Det finnes ingen måte for mottaker å vite om denne filen allerede eksisterte på noden den ble sendt fra eller om den bare ble videresendt fra en annen node og mellomlagret.
Så lenge man ikke kan identifisere alle nodene som lagrer en spesifikk fil er det ikke mulig å få fjernet den.[25]

Sikkerheten til mottaker i Freenet.

Det er viktig at også mottaker kan være anonym, da dette er et nett som har som mål å være en åpen kommunikasjonskanal for alle. I mange tilfeller vil det for den som ønsker å begrense informasjonsflyt, være like interessant å identifisere mottaker som sender. Fordi dette dermed kan være med på begrense den totale ytringsfriheten som er målet for Freenet, er det blitt viktig å hindre slik identifisering.

Siden kommunikasjon via Freenet ikke retter seg mot spesifikke mottakere kan man beskrive mottakers sikkerhet bedre ved å se på nøkkelanonymitet dvs. at det ikke er mulig å finne ut hvilken brukernøkkel som blir etterspurt.

[24] Jonny Egeland, al, Semesteroppgave i TE6013 (2001) s.23.
[25] Jonny Egeland, al, Semesteroppgave i TE6013 (2001) s.5.

Dette er imidlertid umulig i det Freenet-oppsettet som eksisterer i dag fordi ruting av spørringer i Freenet avhenger av at nøkkelen er kjent. Man kan altså tenke seg en mulighet av å spore opp en bruker via en nøkkel.

Det at det brukes krypterte nøkler gir begrenset sikkerhet mot sniklytting på trafikken, men dette kan omgås siden de ukrypterte nøklene må være spredt for at noen skal kunne aksessere filer på Freenet. Såkalte ”dictionary-attacks” vil altså kunne lykkes. Det finnes imidlertid forslag for å gjøre dette bedre. Ved hjelp av noe man kaller pre-ruting skal det kunne gjøres umulig å finne ut både hvor meldingen er sendt fra og hva den inneholder. Dette gjøres ved at Freenet-meldinger krypteres ved hjelp av flere public keys som bestemmer hvor meldingen skal sendes. Man unngår dermed den vanlige rutingen frem til meldingen er dekryptert og den virkelige rutingen begynner. Da er man kommet flere ledd fra noden meldingen ble sendt fra og det er dermed ikke mulig å spore hvor den kom fra. Da det så er umulig å finne avsender er det mindre interessant med hensyn på mottakersikkerhet, om man kan finne ut hva som er sendt. Etter denne pre-rutingen vil vanlig Freenet ruting bli foretatt og meldingen vil være som en melding sendt fra endepunktet for pre-rutingen. [26]

Utgivers sikkerhet.

Når noe skal publiseres på Freenet gjøres dette ved en såkalt insert-request. En insert-request forteller nodene den sendes til at den vil publisere noe på nettet. Når man sender en slik request spesifiserer man også hvor mange ledd videre request’en skal sendes. På denne måten spres informasjonen lengre enn bare til den første noden senderen kontakter. Mellom utgiver og første node (node 1) oppstår et sikkerhetsproblem. Her går informsjonen i klartekst og både innholdet og avsender er dermed ikke skjult for eventuelle ”spioner” som lytter på trafikken lokalt
på node 1.

Det anbefales derfor at man bruker sin egen maskin som node 1 når man publiserer noe. Mellom nodene i Freenet finnes ikke dette problemet fordi her går informasjonen kryptert og det er derfor ”umulig” for lokale lyttere å bestemme hvorvidt en melding fra en annen node oppsto på den aktuelle noden eller bare ble sendt gjennom den.

Ved hjelp av litt mer avanserte teknikker kan likevel sender avsløres. Eksempel: Sett at utgiver A skal publisere et dokument. Han bruker sin egen maskin (node A) som førstenode og unngår dermed at noen snapper opp den ukrypterte informasjonen slik som forklart ovenfor. Etter dette sendes dokumentet videre til node B. På node B prøver man å identifisere utgiveren av denne informasjonen.

[26] Jonny Egeland, al, Semesteroppgave i TE6013 (2001) s.25.

Dette er vanskelig fra en enkeltnode fordi man ikke kan bestemme ut fra dokumentet hvor det kom fra. Dersom node B derimot samarbeider med andre noder og får tilgang til all informasjon som går inn til og ut fra node A blir det enklere. Dersom en av de samarbeidene nodene får en insert-request fra node A og denne ikke har gått inn til node A først kan man konkludere med at requesten må ha sin opprinnelse på node A. Det finnes forslag til måter å lage beskyttelse mot dette i Freenet men det er ikke implementert enda.[27]

Sikkerhet ved flood attacks.

Diskusjonen om fremtiden for FastTrack, OpenNap, Gnutella, iMesh og de andre P2P-nettverkene går høylytt på nyhetsgrupper og chattegrupper på nettet for tiden. Noe er i ferd med å skje. Oftere og oftere viser det seg at sanger og filmer som du laster ned, viser seg å være noe helt annet enn hva du trodde på forhånd.

Det ryktes at store plate- og filmselskaper nemlig i stillhet opprettet store "geriljagrupper" med formål å forurense nettverkene med millioner av falske kopier av populære sanger og filmer. Dermed gjør de det vanskeligere for piratene å finne de ekte filene, og håper at nettverkene i neste omgang vil råtne på rot.
Men på grunn av at filer og data som ligger på Freenet er kryptert og nøkler for å få tilgang til disse filene må være kjent, enten i portaler med oversikt over innhold eller spredd via e-post, brev eller chatte grupper, vil denne type angrep ha liten virkning på Freenet. Det eneste man oppnår er å fylle opp de nærmeste nodene i nettet og det får liten virkning på noder lenger ut i nettet. Skal man kunne lamme Freenet på denne måten må dette gjøres fra mange forskjellige steder. I tillegg må disse dataene etterspørres fra andre steder igjen for å kunne spres videre i nettet for så og holde dem i livet.

Sikkerhet mot fiendtlige noder.

Eksistensen av ondsinnede noder i nettverk er at av de vanskeligste problemene distribuerte nettverk sliter med. Dette har medført undergangen til mange nettverk. Mange nettverkssystem har prøvd å unngå ondsinnede noder med å holde protokoll og koder skjult, men dette har ikke fungert i det lange løp. Freenet har basert seg på åpen kode og det er ikke i tråd med deres filosofi å skjule denne. Freenet har planer om å finne et system for tilbakemelding basert positive og negativ søk mot noder og ut i fra det prøve å unngå de negative noder med å ikke sende spørringer mot dem.[28]

---

[27] Jonny Egeland, al, Semesteroppgave i TE6013 (2001) s.23.
[28] The Freenet Network Project.
http://Freenetproject.org/index.php?page=faq 22.februar, 2005.

Hva inneholder Freenet?

”What`s on Freenet” – en undersøkelse av Dr. Jon Orwant

Dr. Jon Orwant har gjort en undersøkelse på hva som ligger på Freenet. Dr. Jon Orwant er et kjent medlem av Pearl Community, han er en av grunnleggerne av The Perl Journal og har vært med på å skrevet blant annet Programming Perl 3rd Edition. Dr. Jon Orwat`s undersøkelse ble gjennomført i år 2000 altså ganske tidlig i Freenet`s historie. Undersøkelsen heter: ” **What`s On Freenet?** ” og kan leses i sin helhet på denne nettsiden.
http://www.openp2p.com/pub/a/p2p/2000/11/21/Freenetcontent.html .

Men tillatelse fra Dr. Jon Orwant tar vi her et utdrag i fra denne undersøkelsen som kan gi en liten pekepinn på hva som befinner seg på Freenet. [29]

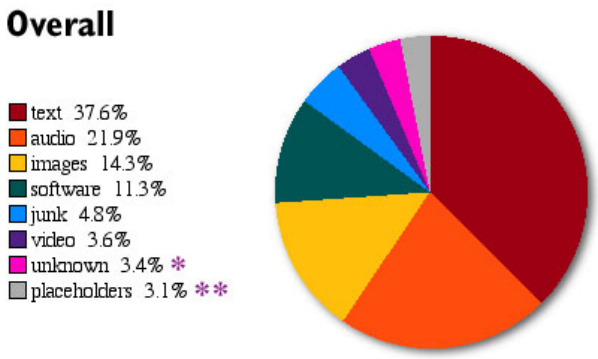
Som nevnt tidligere er Freenet et svært anonymt og kryptert nett som gjør det svært vanskelig å finne ut hva som ligger der uten selv å ta del i evt. spredning av ulovlig materiale. I tillegg må man regne med at en vesentlig del av det som ligger på Freenet ikke er tilgjengelig uten å kjenne til lukkede grupper og deres hemmelige private nøkler. Derfor har vi valgt å bruke denne undersøkelsen selv om den er av en litt eldre årgang.

Måten undersøkelsen ble utført på var å katalogisere alle nøkler som var tilgjengelig i portaler og indekser etter nøkkelnavn og fil typer. På de neste sidene ser vi en grafisk oversikt over de enkelte kategorier.

[29] Med Dr. Jon Orwant tillatelse til bruk og oversettelse av hans artikkel What's on Freenet? epost av 9.mars 2005 (se vedlegg 2) .

Generell samling av innhold:

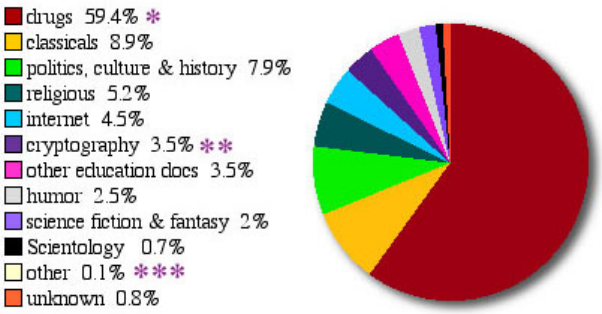
Ut i fra 1075 nøkler ble det funnet disse kategorier av materiale.



*** tilsynelatende** meningsfullt innhold.
****** index over andre linksider.

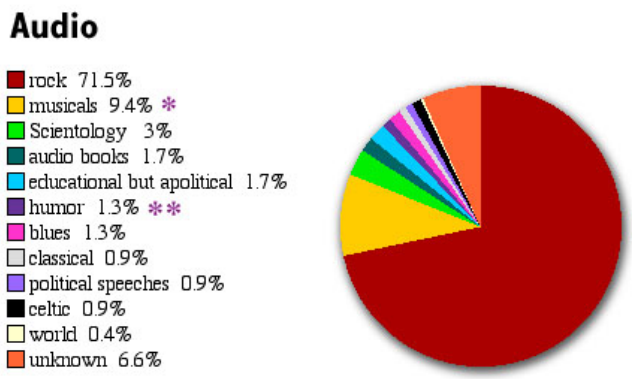
Innhold i kategorien tekst:

19.1 % var tilsynelatende bøker og 80.9 % mer blandet materiale.



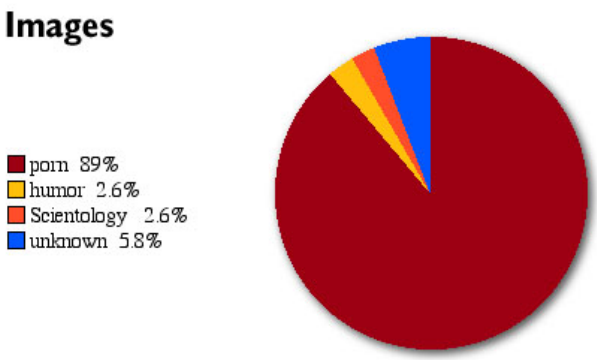
* De fleste av disse ulovlig i USA.
** Inkludert Freenet dokumenter.
*** Copyright materiale.

Innhold i kategorien Audio:



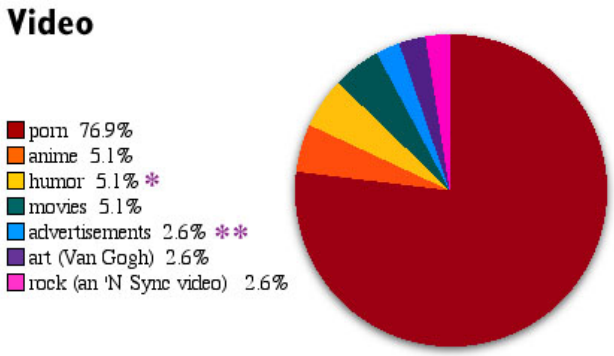
Innhold i kategorien Bilder:

Her presiserer Jon Orwant at alt er kategorisert ut i fra navn på filer og at han har ikke åpnet filene for å se om de inneholder det som står i filbetegnelsen. Blant disse bildene var det en del navn som indikerer at det er bilder av overgrep mot barn.



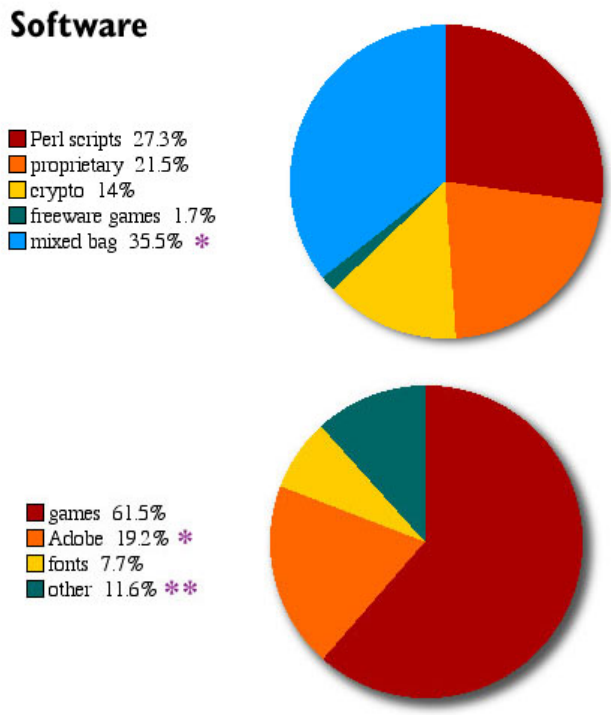
Innhold i kategorien Video:

Her er det ikke nevnt noe om overgrepsmateriale. Men ut i fra dagens Freenet kan man regne med at det også finnes her.



Innhold i kategorien Programvare:

En del scripter og programvare.



Vår konklusjon av undersøkelsen til Dr. John Orwant:

I og med at dette er en gammel undersøkelse og at Freenet på den tiden var relativt ukjent blant den vanlige Internetbrukere, har vi god grunn til å tro at det ligger mye mer ulovlig materiale der nå en for 5 år siden. I de senere år har det blitt fokusert mer på nettsteder med ulovlig innhold, med påfølgende internasjonale aksjoner. Da er det nærliggende å tro at slike grupperinger trekkes til steder som Freenet.

Forsøk på våre to maskiner:

Som en del av vår egen undersøkelse hadde vi installert Freenet på to maskiner og koblet disse opp mot Freenet. Vi gjorde en del forsøk med å legge ut testdokumenter for senere å spørre etter disse.

Vi publiserte en enkel testfil: index.html i Freenetverket og den krypterte URI'en som den siden fikk var:
CHK@ERwzWD~Pdh~5VwYas7sJ936kw68KAwI,emocsTcCu2gLunzwEHoT2A

Og samme filen bare oppdatert noen dager senere ble gitt følgende nøkkel:
CHK@NvETasAPjFEGOy3U5CBZVFTCxLIKAwI,CkDyIIVFCRmCo0RJ6eQLIw

Samme nøkkel brukes for å søke etter filen, og det virker som om en oppdatert fil ikke overskrives men publiseres ut på nytt andre steder i nettverket. Samme filnavn men litt ulik filstørrelse gir en helt ny publiseringsnøkkel. Flere dager etter publiseringen brukte vi nøkkelen for å søke etter filen og websiden som vi hadde publisert noen dager tidligere var i nettverket ennå. Nøkler til sider som bare enkle grupperinger skal ha tilgang til kan utveksles pr e-post, sms, brev, i et forum eller i en irc chattekanal. Utenforstående vil aldri kunne gjette seg til en nøkkel slik at en side forblir "hemmelig" innad i klubben.

Fra vi installerte Freenet overvåket vi mengden data som ble lagret på vår maskin.

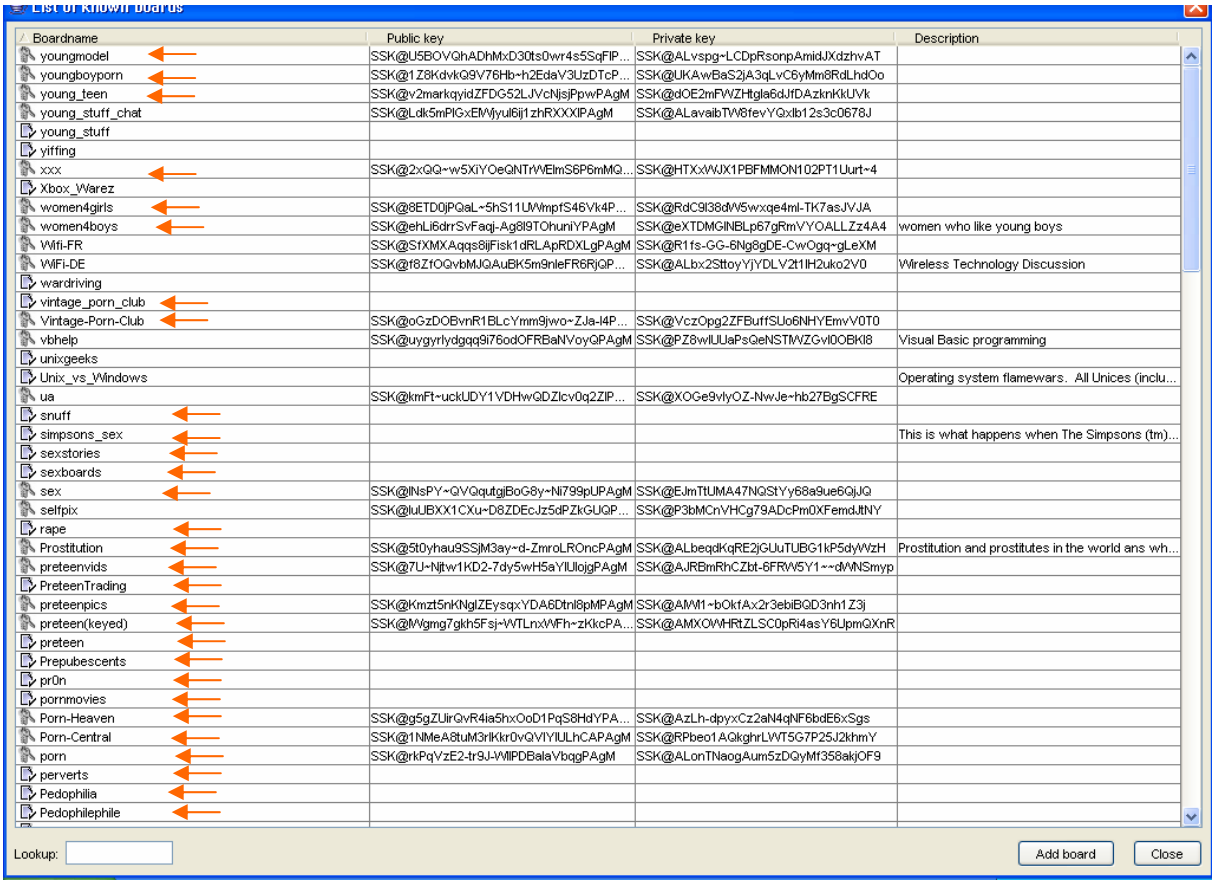
Ved installeringsstart på vår testmaskin var det 862 filer i 461 mapper.

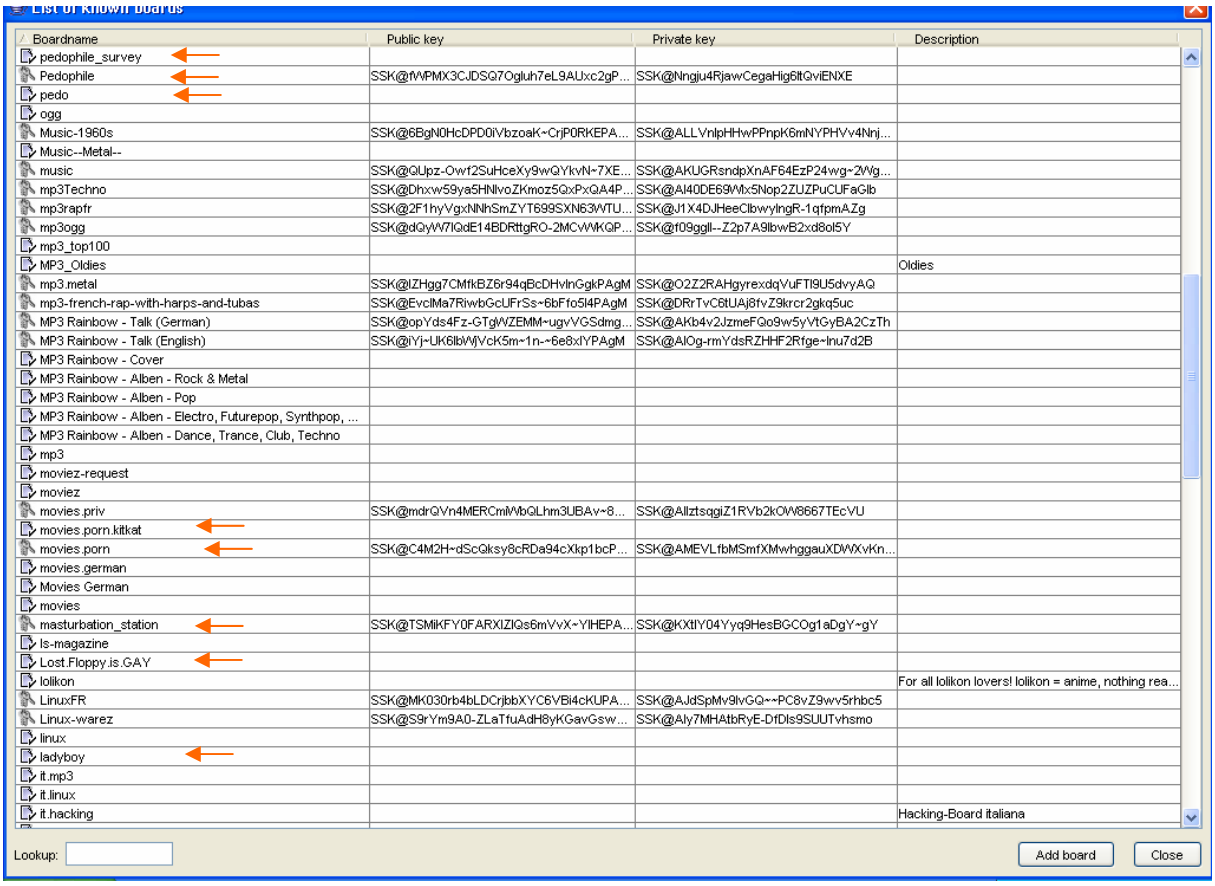
Den 08. mars 2005 var det 936 filer i 471 mapper, på til sammen 26.1 mb. Økningen etter en uke, den 15.mars 2005 var på 1719 filer i 616 mapper, på tilsammen 32.6 mb.

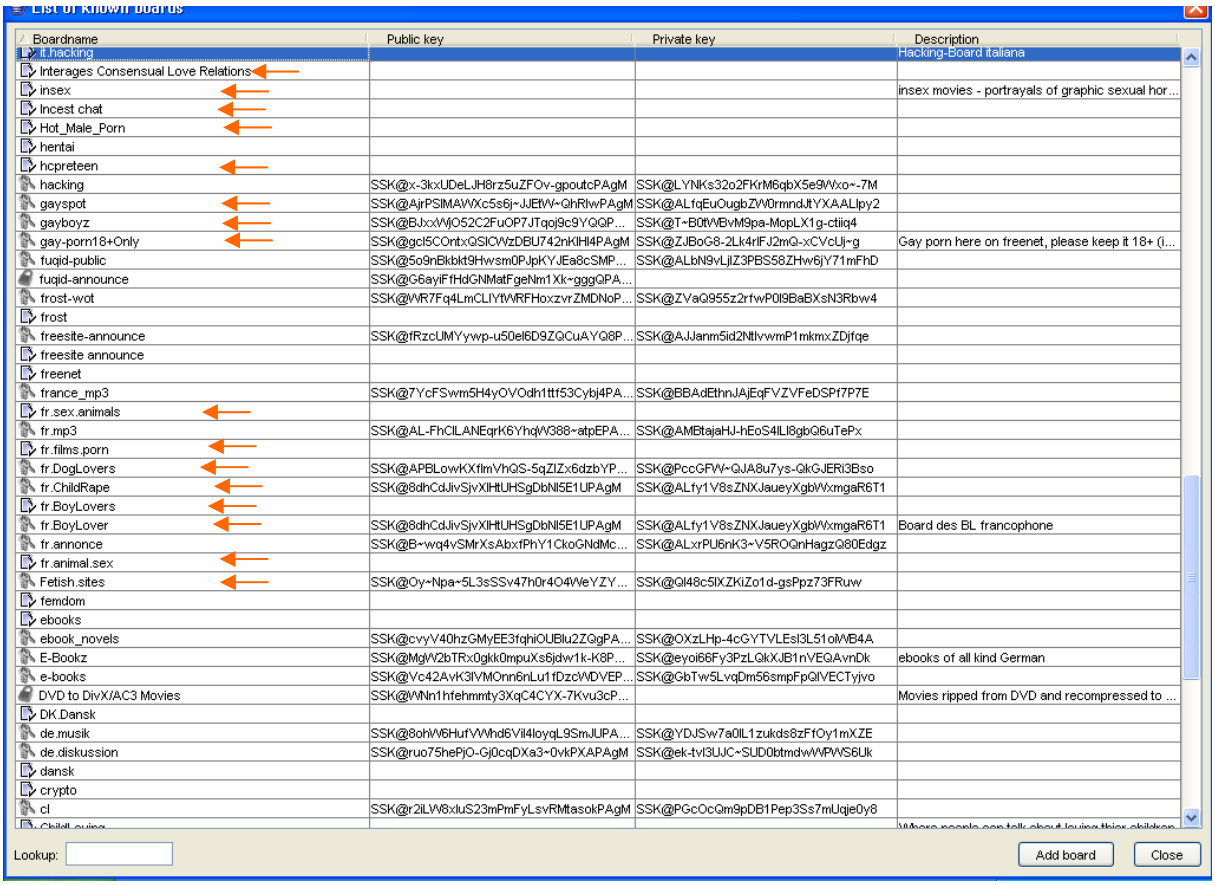
Og dette er filer som er kryptert og vi ikke har noen som helst mulighet å se innholdet av.

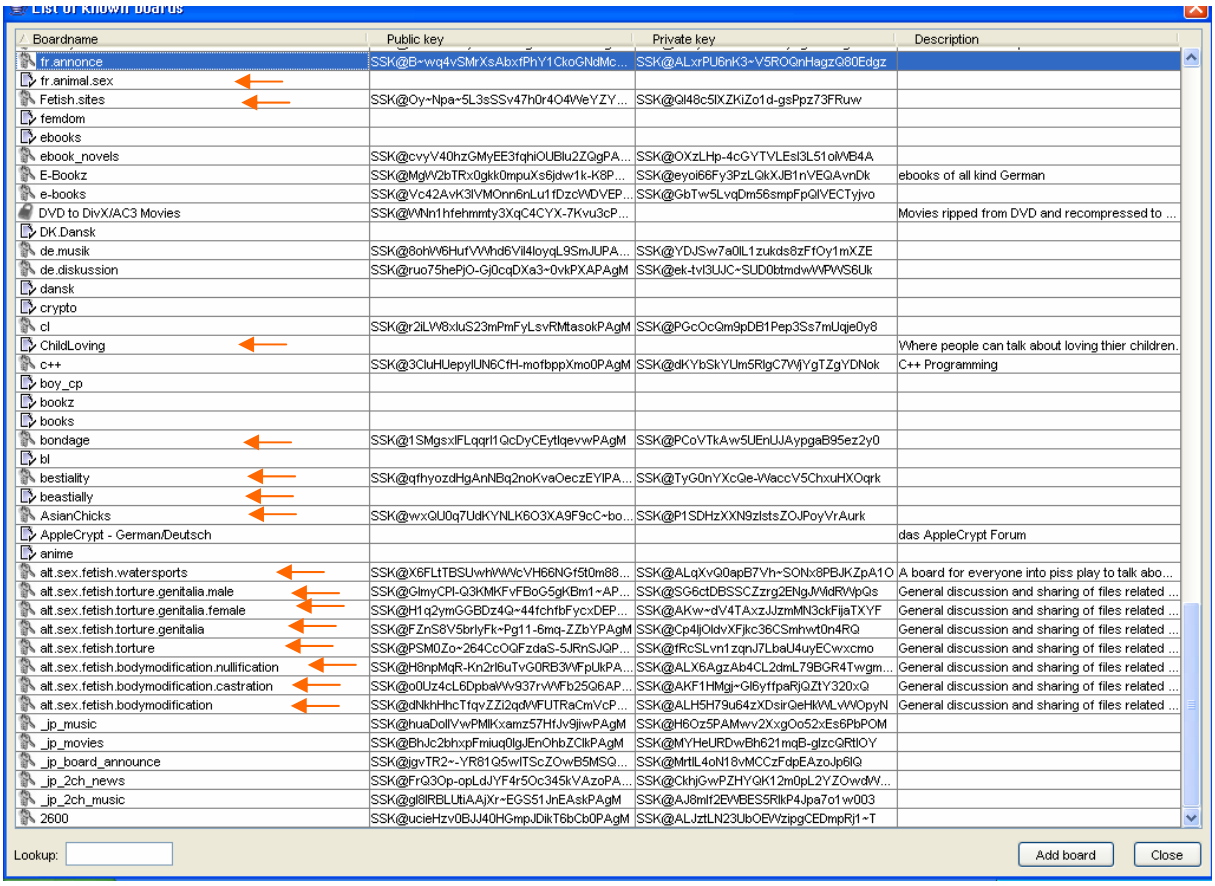
Utskrift fra Freenet.

Skjermdump fra Frost-forum, de med rød pil er forum som man kan anta inneholder pornografisk materiale ut fra beskrivelsen av forumet. Det poengteres at dette er kun en liten del av det man finner og som er ”offentlig” på Freenet. Hva med alt det som holdes hemmelig innenfor lukkede grupper?




List of known boards
Boardname
Public key
Private key
Description
pedophile_survey
Pedophile
SSK@fWPMX3CJDSQ7Ogluh7eL9AUxc2gP...
SSK@Nngju4RjawCegaHig6ltGviENXE
pedo
ogg
Music-1960s
SSK@6BgN0HcDPD0iVbzoaK~CrjP0RKEPA...
SSK@ALLVnlpHHwPPnpK6mNYPHVv4Nnj...
Music--Metal--
music
SSK@QUpz-Owf2SuHceXy9wQYkvN~7XE...
SSK@AKUGRsndpXnAF64EzP24wg~2Wg...
mp3Techno
SSK@Dhxw59ya5HNlvoZKmoz5QxPxQA4P...
SSK@AI40DE69Wx5Nop2ZUZPuCUFaGlb
mp3rapfr
SSK@2F1hyVgxNNhSmZYT699SXN63VTU...
SSK@J1X4DJHeeClbwylngR-1qfpmAZg
mp3ogg
SSK@dQyW7lQdE14BDRttgRO-2MCvWKQP...
SSK@f09ggll--Z2p7A9lbwB2xd8ol5Y
mp3_top100
MP3_Oldies
Oldies
mp3.metal
SSK@lZHgg7CMfkBZ6r94qBcDHvlnGgkPAgM
SSK@O2Z2RAHgyrexdqVuFTl9U5dvyAQ
mp3-french-rap-with-harps-and-tubas
SSK@EvclMa7RiwbGcUFrSs~6bFfo5l4PAgM
SSK@DRrTvC6tUAj8fvZ9krcr2gkq5uc
MP3 Rainbow - Talk (German)
SSK@opYds4Fz-GTgWZEMM~ugvVGSdmg...
SSK@AKb4v2JzmeFQo9w5yVtGyBA2CzTh
MP3 Rainbow - Talk (English)
SSK@iYj~UK6lbWjVcK5m~1n-~6e8xlYPAgM
SSK@AIOg-rmYdsRZHHF2Rfge~lnu7d2B
MP3 Rainbow - Cover
MP3 Rainbow - Alben - Rock & Metal
MP3 Rainbow - Alben - Pop
MP3 Rainbow - Alben - Electro, Futurepop, Synthpop, ...
MP3 Rainbow - Alben - Dance, Trance, Club, Techno
mp3
moviez-request
moviez
movies.priv
SSK@mdrQVn4MERCmlVbQLhm3UBAv~8...
SSK@AllztsqgiZ1RVb2kOW8667TEcVU
movies.porn.kitkat
movies.porn
SSK@C4M2H~dScQksy8cRDa94cXkp1bcP...
SSK@AMEVLfbMSmfXMwhggauXDWXvKn...
movies.german
Movies German
movies
masturbation_station
SSK@TSMlKFY0FARXIZlQs6mVvX~YlHEPA...
SSK@KXtlY04Yyq9HesBGCOg1aDgY~gY
ls-magazine
Lost.Floppy.is.GAY
lolikon
For all lolikon lovers! lolikon = anime, nothing rea...
LinuxFR
SSK@MK030rb4bLDCrjbbXYC6VBi4cKUPA...
SSK@AJdSpMv9lvGQ~~PC8vZ9wv5rhbc5
Linux-warez
SSK@S9rYm9A0-ZLaTfuAdH8yKGavGsw...
SSK@Aly7MHAtbRyE-DfDls9SUUTvhsmo
linux
ladyboy
it.mp3
it.linux
it.hacking
Hacking-Board italiana
Lookup:
Add board
Close


List of known boards
Boardname
Public key
Private key
Description
it.hacking
Hacking-Board italiana
Interages Consensual Love Relations
insex
insex movies - portrayals of graphic sexual hor...
Incest chat
Hot_Male_Porn
hentai
hcpreteen
hacking
SSK@x-3kxUDeLJH8rz5uZFOv-gpoutcPAgM
SSK@LYNKs32o2FKrM6qbX5e9Wxo~-7M
gayspot
SSK@AjrPSlMAWXc5s6j~JJEtW~QhRlwPAgM
SSK@ALfqEuOugbZW0rmndJtYXAALlpy2
gayboyz
SSK@BJxxWjO52C2FuOP7JTqoj9c9YQQP...
SSK@T~B0tWBvM9pa-MopLX1g-ctiiq4
gay-porn18+Only
SSK@gcl5COntxQSlCWzDBU742nKlHl4PAgM
SSK@ZJBoG8-2Lk4rIFJ2mQ-xCVcUj~g
Gay porn here on freenet, please keep it 18+ (i...
fuqid-public
SSK@5o9nBkbkt9HwsmQPJpKYJEa8cSMP...
SSK@ALbN9vLjlZ3PBS58ZHw6jY71mFhD
fuqid-announce
SSK@G6ayiFfHdGNMatFgeNm1Xk~gggQPA...
frost-wot
SSK@WR7Fq4LmCLIYfWRFHoxzvrZMDNoP...
SSK@ZVaQ955z2rfwP0l9BaBXsN3Rbw4
frost
freesite-announce
SSK@fRzcUMYywp-u50el6D9ZQCuAYQ8P...
SSK@AJJanm5id2NtlvwmP1mkmxZDjfqe
freesite announce
freenet
france_mp3
SSK@7YcFSwm5H4yOVOdh1ttf53Cybj4PA...
SSK@BBAdEthnJAjEqFVZVFeDSPf7P7E
fr.sex.animals
fr.mp3
SSK@AL-FhClLANEqrK6YhqW388~atpEPA...
SSK@AMBtajaHJ-hEoS4lLl8gbQ6uTePx
fr.films.porn
fr.DogLovers
SSK@APBLowKXflmVhQS-5qZIZx6dzbYP...
SSK@PccGFW~QJA8u7ys-QkGJERi3Bso
fr.ChildRape
SSK@8dhCdJivSjvXlHtUHSgDbNl5E1UPAgM
SSK@ALfy1V8sZNXJaueyXgbWxmgaR6T1
fr.BoyLovers
fr.BoyLover
SSK@8dhCdJivSjvXlHtUHSgDbNl5E1UPAgM
SSK@ALfy1V8sZNXJaueyXgbWxmgaR6T1
Board des BL francophone
fr.annonce
SSK@B~wq4vSMrXsAbxfPhY1CkoGNdMc...
SSK@ALxrPU6nK3~V5ROQnHagzQl80Edgz
fr.animal.sex
Fetish.sites
SSK@Oy~Npa~5L3sSSv47h0r4O4WeYZY...
SSK@Ql48c5lXZKiZo1d-gsPpz73FRuw
femdom
ebooks
ebook_novels
SSK@cvyV40hzGMyEE3fqhiOUBlu2ZQgPA...
SSK@OXzLHp-4cGYTVLEsl3L51olWB4A
E-Bookz
SSK@MgW2bTRx0gkk0mpuXs6jdw1k-K8P...
SSK@eyoi66Fy3PzLQkXJB1nVEQAvnDk
ebooks of all kind German
e-books
SSK@Vc42AvK3lVMOnn6nLu1fDzcWDVEP...
SSK@GbTw5LvqDm56smpFpQlVECTyjvo
DVD to DivX/AC3 Movies
SSK@WNn1hfehmmty3XqC4CYX-7Kvu3cP...
Movies ripped from DVD and recompressed to ...
DK.Dansk
de.musik
SSK@8ohW6HufVWnd6Vil4loyqL9SmJUPA...
SSK@YDJSw7a0lL1zukds8zFfOy1mXZE
de.diskussion
SSK@ruo75hePjO-Gj0cqDXa3~0vkPXAPAgM
SSK@ek-tvI3JJC~SUD0btmdvWPWS6Uk
dansk
crypto
cl
SSK@r2iLW8xluS23mPmFyLsvRMtasokPAgM
SSK@PGcOcQm9pDB1Pep3Ss7mUqje0y8
Lookup:
Add board
Close



Som man ser ut i fra beskrivelsene av nøklene over er en betydelig del av det som ligger på Freenet relatert til porno og bilder av seksuelle overgrep mot barn. En kan bare anta at dette er en liten del av det som finnes her.

Analyse.

Distribusjon og sporing av overgrepsbilder?

Nå som Freenet antakelig er blitt kjent som et sted der man kan opptre anonymt og ikke frykte represalier eller forfølgelse fra myndigheter eller andre, er dette også et mulig fristed for utveksling av overgrepsmateriale. Her kan lukkede grupper og miljøer opprette skjulte grupper / nettverk og operere relativt trygt og skjult fra resten av omverden.

I følge undersøkelsene og de opplysninger som vi har vist ovenfor mener vi at det er bortimot en håpløs oppgave for myndighetene å kunne kontrollere hva som skjuler seg på Freenet. Selv om en skulle klare å infiltrere seg i disse skjulte gruppene vil det være en nesten umulig oppgave å spore opp hvem som er kilde til det materialet som ligger der.

Vi mener likevel ikke at det er helt umulig, men det vil kreve enorme resurser og et nitidig arbeid å dekryptere den informasjonen en måte finne. Med dagens resurser innenfor kampen mot seksuelle overgrep mot barn ser vi dette som en håpløs oppgave. Spørsmålet er om man får myndighetene i de enkelte land med på å satse så store resurser.

Vi kan ikke se at selve Freenet-konseptet er ulovlig i seg selv, men en kan stille seg spørsmålet om vi ”vanlige” mennesker er tjent med et slikt fristed.

Den enkelte bruker bør gjøre en vurdering av eget moralsk ståsted før han/hun bruker Freenet.

Anonymiteten og ytringsfriheten på Freenet har sin pris.

Er du villig til å dele resurser på din egen datamaskin for at andre skal kunne lagre informasjon som du ikke kan se og dermed indirekte kan være med på å distribuere ulovlig materiale?

Juridisk er det også interessant, med tanke på tidligere rettsavgjørelser i forbindelse med overgrepsbilder i datamaskinens ”cache”. Hvis man ikke kan dømmes for besittelse av overgrepsbilder man måtte ha liggende i nettleserens mellomlager, hva da med overgrepsmateriale som er kryptert og ligger på en lagerplass tilordnet Freenet, og som man kan påstå man ikke hadde anelse om med henvisning til Freenet sitt system med mellomlagring av filer på alle noder i nettet?

Avsluttende Konklusjon.

Kampen om det frie Internett.

Internett er internasjonalt, og blir av mange sett på som verdens største anarki. Ingen eier nettet, og ingen bestemmer over Internett i sin helhet. Det er et råd av sentrale aktører, men ingen egentlig myndighet. Hvordan skal da kommunikasjon på nettet lovreguleres, og hvordan kan nettet bli styrt best mulig? Fordi informasjonen overføres over landegrensene, blir problemet også hvilke lands lover som skal anvendes. Dette er et aktuelt spørsmål verden over, og derfor er det mange forskjellige formeninger om denne internasjonale kommunikasjonsformen. De fleste land er bygd opp etter forskjellige rettsapparater, og av den grunn mange forskjellige syn på hva som er rett og galt. Hvor skal grensen settes for hva som skal ytres og distribueres via nettet?

Her kommer problematikken inn. Nettet uten grenser blir misbrukt til å spre rasisme, pornografi, seksuelle overgrep mot barn og dette har en skremmende effekt. Hva skal man godta, og hvor skal man sette grensene?
Ved å sensurere «Internet», vil den nye kommunikasjonsteknologien sprenge sensurens ramme fordi utviklingen av teknologien vil tvinge frem en ny informasjonsfrihet slik som den vi ser i Freenet.

Kristelig Folkepartis Kjell Magne Bondevik savner et internasjonalt regelverk som kan sette en sperre for dette. Dette virker veldig enkelt i teorien, men hvordan vil dette fungere i det virkelige liv? Sensurkritikerne mener det ikke er mulig å bruke internasjonal lovgivning på Internett rettet mot innholdet, for det kan gå mot vår ytringsfrihet. Men hva er akseptabel ytringsfrihet og hva er uakseptable lovbrudd?

Alle norske lover gjelder den norske delen av Internett, og Norges lover inneholder paragrafer som verner enkeltindivider (for eksempel loven om personvern, og straffeloven) Disse lovene gjelder derfor også Internettbruken i Norge, og omfatter nordmenns bruk av Internett uansett hvor de befinner seg.

Men hva hjelper det når det i deler av verden hersker anarki på Internett og aktører opererer fritt i land hvor lovverket er mangelfullt?

Med basis i et slikt bakteppe, og med grunnlag i bruken av sterk kryptering av alle data – hvordan kan man da kontrollere bruken av Freenet?

En operasjon av typen Enea er i alle fall utelukket, slik vi ser det.

Analyse av FreeNet

Obligatorisk oppgave 1 i Samfunnsinformatikk

ved

HiNe

Våren-2005

Utarbeidet av: Gruppe **E**

Bestående av:

Roy Thoresen

Ole-Jonny Johansen

Historie og Konsept

"I juli 1999 startet den Irske informatikkstudenten Ian Clarke (IC) et prosjekt som omhandlet open-source (åpen-kilde), dette prosjektet kalles ”A Distributed Decentralised Infomation Storage and Retrival System”.[30] Og det er han som i dag koordinerer prosjektet som vi i dag kaller for Freenet.

1.1 Systemet

Han ville lage et system som skulle være 100 % motstandsdyktig mot sensur, han så for seg et system hvor dokumenter kunne publiseres og leses fritt, uten at disse dokumentene kunne spores tilbake til en bestemt fysisk og geografisk lokaliserbar adresse. Freenet var ikke ment som et alternativ til Internett men heller som et nettverk med dokumenttjenere som kjører på Internettmaskiner [31]. De som kjører Freenet-tjenere, gjør det på frivillig basis, og de kan ikke få vite hvilke dokumenter som er lagret på deres maskin. Dokumentene og deres plassering er beskyttet med sterk kryptering. Dersom noen prøver å finne ut lokaliseringen til et dokument, skulle det kopieres videre til flere andre Freenet-tjenere. Slik motarbeider Freenet automatisk og aktivt ethvert forsøk på kontroll. Jo flere forsøk på sensur, desto mer redundans. Det er en direkte linje fra Shannons[32] informasjonsteori (Informasjonsteknologienes far) til informatikkstudenten Clarke praksis. I og med at Clarke har benyttet seg av Shannons teori om bruken av matematikk for å få krypteringen som brukes i Freenet til å fungere.

---

[30] ”(Et distribuering desentralisert informasjon lagring og gjenfinnings system)” www.freenetproject.org

[31] Internettmaskiner:er andre brukeres maskiner som også kjører Freenet. Også kalt ”noder” http://java.sun.com/j2se/1.4.2/docs/api/org/w3c/dom/Node.html

[32] Claude Shannon rangerer blant de tre som har betydd mest for IT-utviklingen. Uten ham - intet Napster, intet Internett, ingen overføring av bilder fra fjerne planeter.
Claude Shannons arbeid var banebrytende når det gjaldt å forstå informasjon som konsept. Han beskrev sine teorier i to avhandlinger som kom i henholdsvis 1938 og 1948. Teoriene kan nok være kjent for de fleste, men hvordan de ble til, er nok ikke like kjent. Men til gjengjeld fascinerende eksempler på hvordan vitenskapen gjør sine fremskritt.
Men det Shannon så var at de elektriske kretsene kunne åpnes og lukkes ved hjelp av en elektromagnet. Han kombinerte denne observasjonen med et annet studium han hadde tatt innen språkfilosofi, nemlig symbolsk logikk - et utsagn var enten sant eller falskt. Hvorfor ikke overføre dette på elektronikk - en elektrisk krets var enten på eller av, symbolisert ved tallene 1 og 0?
Shannons bidrag var å vise at ethvert logisk utsagn - hvor komplisert det enn var - kunne uttrykkes ved hjelp av et nettverk av enkle koblinger. Enda viktigere - slike utsagn kunne også foreta sammenligninger: "Hvis tallet X er lik tallet Y, utfør da operasjon V". Konsekvensene av dette var store - det betød at en maskin kunne ta avgjørelser basert på "enkel" symbolsk logikk.
http://www.digi.no/digi98.nsf/pub/dd20011008120323__10325474
http://www.nyu.edu/pages/linguistics/courses/v610003/shan.html

1.2 Idealistene

Det var flere idealister som hang seg på konseptet, deriblant Oskar Sandberg[33] som var blant de første som bidro til prosjektet og fortsatt bidrar og har en hovedrolle i utviklingen av systemet. Man har også Scott Miller[34] som har ansvaret med innleggingen av data og mye av krypteringen, Matthew Toseland[35] som har bidratt nesten helt fra begynnelsen og hans arbeid har resultert i at det har vært en dramatisk forbedring av systemet når det gjelder ytelse og stabiliteten til systemet, Steven Starr[36] som koordinerer det økonomiske aspektet med Freenet og mange andre folk som har gode kunnskaper innen programmering og utvikling[37].

1.3 Utvikling

Systemet er laget slik at det hele tiden er under utvikling. Freenets skapere oppfordrer til at de som vil kan være med på videreutviklingen av systemet. På samme måte som andre idealistiske konsepter som Linux etc. Hvis noen kommer med en bedre løsning på et gitt problem blir dette tatt opp til vurdering av de andre i Freenet organisasjonen. Da de har som mål å hele tiden utvikle produktet til det bedre.

1.4 Økonomi

Konseptet er også basert økonomisk på gaver, sponsorer og salg av support artikler for at det i hele tatt skal være økonomisk grunnlag for å drive systemet, da ideologien er at det skal være et non profitt selskap (det skal altså ikke være lønnsomt).

1.5 Mål

Målet til utviklerne av Freenet er å fremme ytringsfriheten til folk som bor i land hvor det kan bli et verktøy for mennesker uten fri meningsflyt (Kina, Nord-Korea, Burma og land i Midtøsten, etc.)[8]

---

[33] Oskar sandberg: Ph.d. I matematisk statistikk.
http://www.math.chalmers.se/~ossa/
[34] Scott Miller:
Scott Miller is a senior software developer for Uprizer, Inc. and a core developer with Freenet since 2000. Miller has a B.S. with honors from Indiana University
http://conferences.oreillynet.com/cs/p2pweb2001/view/e_spkr/563
[35] Mattew Toseland Jobber fulltid I Freenet
http://www.freenetproject.org/
[36] Steven Starr:
Koordinator i Freenet.
http://www.ominous-valve.com/pac/archive/020125starr_imc.html
http://www.savepacifica.net/20020126_schubb.html
[37] De andre
http://www.freenetproject.org/papers/freenet-ieee.pdf

1.6 I dag

Det er lenge siden Freenet forlot forskningsstadiet på laben. Det har blitt nedlastet av over 2 millioner brukere siden prosjektet startet, det blir i dag foretatt ca: 3000 nedlastinger av programvaren hver dag (nye brukere). Det blir brukt til distribusjon av kryptert materiale/info over hele verden. [38]

Intensjonen bak Freenet

Intensjonen for kjernen av Freenets utviklere har hele tiden vært basert på ønske om å få laget et forum/system der folk kan ytre sine meninger uten at de skal kunne bli forfulgt, overvåket eller straffet for sine meninger.

De har i sitt arbeide med design av systemet fokusert på:

- ”Anonymitet for de som publiserer, forbrukere eller rettighetshavere
- Motstand mot sensurering
- Høy tilgjengelighet og pålitelighet gjennom desentralisering av nettverket (nodene).
- Effektivitet, målbarhet og tilpassningsdyktighet for lagring og routing” [10].

2.1 Kommunikasjon

Det de legger mest vekt på er friheten til å kommunisere, da det er en fundamental rettighet i et demokratisk samfunn. De har ingen mulighet til å nekte de personene med ”dårlige hensikter” uten å måtte stenge ute personer med ”gode hensikter”, menneskerettighets aktivister, minoritets grupper, religiøse grupper eller andre ordinære personer som ønsker at deres aktivitet ikke er noen offentlig anliggende.

2.2 Anonymitet

For å opprettholde anonymiteten til de som publiserer og laster ned filer så er det også viktig at filene i seg selv også har den samme anonymitet og beskyttelse mot angrep (”attack”).

---

[38] Hva er på Freenet i dag?
http://www.itic.ca/DIC/News/2004/05/freenet_TOP10_countries.jpg
http://www.openp2p.com/pub/a/p2p/2000/11/21/freenetcontent.html
[10] Kilde: www.freenetproject.org

De har derfor gjort det svært vanskelig for å oppdage eksakt hvilken datamaskin (datastore) filen ligger på, sammen med overflødige kopier av data. Den som har data lagret anonymt gjør det ekstremt vanskelig for noen å sensurere eller ødelegge filene som ligger lagret i nettverket.

2.3 Lagring

Freenet prøver ikke å garantere for permanent lagring av data, fordi lagringsplassen er begrenset, men utvekslingen av data eksisterer mellom publisering av nye filer og ivaretaking av gamle filer. Mange systemer løser dette problemet med å ta betaling i form av plass på harddisken eller penger, men Freenet vil heller oppfordre til publisering, heller enn å måtte avise de som ikke har muligheter til å kjøre et fildelingssystem eller er for fattige til å betale for lagringen.

Mulighetene for å holde søppel filer fra å fylle opp all tilgjengelig lagrings plass eller overskrive eksisterende data. Her har Freenet laget en fremgangsmåte som de håper at brukerne vil samle tilstrekkelig nok ressurser som kan ivareta filenes opprinnelse på ubestemt tid.

2.4 Blokkering

Menneskerettsorganisasjoner (Human Rigth Watch) og det Globale Internett frihets kampanje har dokumentert at myndighetene rundt om i verden forsøker å tvinge Internett leverandørene til å blokkere tilgangen til innholdet som er upassende, straffbart og ødeleggende eller prøver å gjøre dem ansvarlig for slikt materiale på sine servere[11].

2.5 Personvern

The Electronic Privacy Information Center (TEPIC)[12] har også stilt spørsmål om ytringsfrihet og personvern. Angående utviklingen av Federal Bureau of Investigasjons (FBI) og Europa Unionens (EU) nye systemer[13] som gir myndighetene muligheter til å overvåke og kartlegge trafikken av elektroniske overføringer av data via Internett.

---

[11] http://hrw.org/advocacy/internet/
http://www.gilc.org/
http://www.google.com/search?hl=no&q=Human+Rights+Watch%2BInternett&lr
http://www.freenetproject.org/papers/freenet-ieee.pdf

[12] http://www.freenetproject.org/papers/freenet-ieee.pdf
http://www.epic.org/

[13] Carnivore electronic monitoring system and the European Union's new "Convention on Cybercrime," which gives authorities broad powers to intercept and record digital Communications. http://www.freenetproject.org/papers/freenet-ieee.pdf

Selv om det tilsynelatende filtrerer ut eller forebygger sensurering og opprettholder den privates fundamentale rett til fritt å kunne uttrykke/uttale seg i en potensiell farlig verden, og ivareta muligheten til å publisere kontroversiell informasjon så er dette bare halve problemet.

Enkelt personer kan ofte bli offer for personlig forfølgelse for å ha og publisert eller lest slikt materiale[14], og de kan bli nødt til å skjule sin identitet for å unngå å bli forfulgt. Til og med Amerikansk Høyesterett har lenge sett viktigheten av å kunne utale seg anonymt om politiske spørsmål på Internett[15].

2.6 Verktøy for kriminelle

Et vanlig argument for å sikre/overvåke kommunikasjon er at kriminelle kan bruke det til å begå kriminelle handlinger[16]. Freenet er ikke så veldig attraktiv for slike handlinger i og med at det kun er laget for å publisere innhold, og dermed ikke til å godt egnet for hemmelige kriminelle komplott[17] slik som terror, ran, narkotika og overgrepsbilder. Likevel, elektronisk kommunikasjon er jo bare tross alt et verktøy, de kan jo bare benytte seg av offentlige telefon automater, anonyme mobiltelefoner eller vanlig brev i gjennom posten, for å utføre sine handlinger uavhengig om intensjonen er god eller dårlig.

En terrorist kan bruke det til å planlegge et angrep, han kan publisere handlingen han har tenkt å utføre på Freenet sine sider og dermed koordinere angrepet med de andre terroristene, eller en informant kan bruke det til å angi terroristen til myndighetene. Informanten kan lese dette på Freenet hvis han forespør slikt materiale og deretter varsle myndighetene.

---

[14] Materiale som den enkelte myndighet ser på som lovstridig. Og eventuelt truende mot det politiske system

[15] the U.S. Supreme Court, among others, has long recognized the important
Role of anonymous speech in political dissent.
http://www.supremecourtus.gov/
http://www.freenetproject.org/papers/freenet-ieee.pdf

[16] Handlinger som defineres som straffbart I følge lovverket/grunnloven til det eller de respektive landene som handlingen utføres i.

[17] Planlegging av en kriminell handling (planlegging av en handling som strider mot lovverket).

Hva er Freenet

3.1 Nettverket

Freenet er et nett i nettverket (Internett) der det ikke skulle være mulig for andre å se hva som ble lest og hvem som hadde laget produktet, altså et nettverk der ”storebror”(myndighetene og andre lovgivende organer ikke hadde mulighet for sensur og overvåking).
Men det kan ikke sammenlignes med www (WorldWideWeb). Freenet er et slags peer2peer (fildelings system) men med en helt annen intensjon og virkemåte enn det som er med et vanlig fildelingssystemer på som for eksempel: napster og andre fildelings systemer som er linket (bundet) til en fast fysisk server. Nettverket distrubierer informasjon etter hvor populær den er, og benytter seg av noder (maskinene til andre brukere og deres egne maskiner) for å lagre informasjonen som er tilgjengelig på Freenet, altså ikke på en fast fysisk server, de som blir med i Freenet må/kan fristille plass på harddisken til maskinene sine, også kalt datastore, de må også dele bandwith (båndbredde/hastighet) med de andre brukerne, slik at deres egen hastighet blir svekket, du låner altså ut båndbredde og lagringsplass til de andre brukerne.
Alt som blir publisert i /på Freenet er tungt kryptert og særdeles vanskelig å dekode.

3.2 Virkemåte

Freenet er et gratis program som lar deg publisere og oppnå/få/erverve informasjon på Internett uten fare for sensur. For å oppnå denne friheten er nettverket helt desentralisert og de som ønsker å publisere eller bruke informasjonen er anonyme. Uten anonymitet kan det aldri bli full ytringsfrihet og uten desentraliseringen av nettverket vil det være utsatt for skadelige angrep. Kommunikasjonen mellom brukere i nettverket er kryptert, og det blir lagt litt av data/filer på forskjellige nodene for å gjøre det ekstremt vanskelig for å vite hvem som forespør etter informasjon og hva informasjonen inneholder. Ulikt andre fildelings systemer lar Freenet ikke andre bruker kontrollere hva som er lagret i datastoren, i stedet er filene bevart eller blir slettet alt etter hvor populær forespørselen er etter filene. Filer som ikke er populære blir som regel slettet etter en stund for å gi plass til nyere og mer populært innhold. Filene i datastoren er kryptert for å redusere sannsynligheten for tiltale/forfølgelse av personer som måtte inneha disse data.
Nettverket kan bli brukt til flere forskjellige måter og er ikke begrenset til bare deling av filer slik som andre fildelings systemer, det virker mer som et slags Internett i Internett. Det kan blant annet brukes til publisering av hjemmesider (”freesites”), kommunikasjon ved hjelp av pratekanaler (chat) osv.

Arkitekturen og virkemåte til Freenet

Systemet er bygd opp som et tre eller som en pyramide, der brukeren som er mest aktiv og har mest forespørsler og eller publiserer og lagrer mest vill få økt hastighet og økt tilgang til materialet/data som bruker forespør, altså den ”rike blir rikere” og den ”rike” kan regnes som stammen i et tre der informasjonen er mest tilgjengelig for stammen kontra de som er greiner eller blad som da må bruke lenger tid for å få tilgang til data.

Kryptering

Som sagt tidligere er alt av innholdet i Freenet arkitekturen tungt kryptert, og for å få en bedre forståelse av dette skal vi prøve å forklare hvordan denne krypteringen funger.

5.1 Hashing

De bruker hovedsakelig Hashing til kryptering Figurativt så betyr Hash: virvar, rot, røre. La oss ta et eksempel: Vi kunne ha tenkt oss at vi har tatt alle bokstaver som står i denne rapporten og skrevet hver enkelt bokstav på en lapp, deretter så har vi lagt alle disse lappene i en stor eske og blandet dette godt. Så har vi tømt alle disse lappene med bokstaver utover på gulvet for så å sette disse sammen slik at de ble sammenhengene ord og linjer. Dette vil jo så å si være umulig da i hvert fall og fått dette eksakt lik slik det var i utgangspunktet. Vi hadde helt sikkert klart og sette sammen ord men neppe på en måte slik at dette ble sammenhengene og hele forklarende setninger.

I datasammenheng så vil man kunne gjøre det samme men da gitt at systemet vet hvordan dette ble blandet på for så og sette dette sammen igjen. Man må da lage en nøkkel for å håndtere dette. Og den som sitter med nøkkelen får dette gjort mens den som ikke innehar en nøkkel vil heller ikke kunne gjøre dette. Man trenger riktig nøkkel for og åpne rett dør.

Hash er en måte og kryptere filer på. Måten dette gjøres på er og omgjøre de naturlige tegn/siffer til koder bestående av tall og bokstaver som blir satt sammen i en uforstående rekkefølge slik at det blir en streng av dette. Kjennetegnet til en hashfunksjon er at den alltid vil produsere samme resultat når den jobber mot en og samme tekststreng. Dette er tung mattematikk og enkelte krypteringer er så å si helt umulig og dekryptere. Det finnes enklere Hash funksjoner som ofte brukes til å kryptere passord eks: pinkode. Så det som blir gjort i Freenet er at hver fil vil få sin egen kode

5.2 Kryptografi

”Kryptografi er en tusen år gammel metode for å skjule innhold i en skriftlig meddelelse. De første krypteringsmetodene benyttet f.eks. enkle algoritmer (beregningsmetoder) som gikk ut på å forskyve bokstavene i alfabetet et visst antall plasser”[18].

For å kunne lese (dekryptere) et skjult innhold, trengte mottakeren en nøkkel. Nøkkelen fortalte hva som måtte gjøres for å få fram den opprinnelige teksten. En nøkkel for tekst kryptert etter algoritmen nevnt over, kunne være 3H, som betydde at forskyvingen av alfabetet var 3 bokstaver mot høyre.

Moderne kryptografi benytter avanserte matematiske funksjoner for å forvrenge innhold i dokumenter og meldinger. Moderne kryptografi er avhengig av datamaskiner for å fungere.

Det finnes to hovedtyper kryptografiske metoder som benyttes i dag:

- Symmetrisk kryptografi (det samme som chk-nøkkel i Freenet).
- Asymmetrisk kryptografi (det samme som ssk-nøkkel i Freenet).

Navnene på disse metodene henspiller på hvordan nøklene brukes i hver av dem.

5.3 Symmetrisk kryptografi

Baserer seg på samme grunnleggende metode som for tusen år siden. Avsenderen og mottakeren av en kryptert meddelelse må ha den samme nøkkelen for å kryptere og dekryptere teksten.

Dette skaper problemer mht. å distribuere nøkkelen til alle som behøver å ha den for å kunne dekryptere hemmelige meddelelser. Faller nøkkelen i hendene på uvedkommende, kan den hemmelige meldingen leses av dem. De som samhandler, må bl.a. skaffe seg en ny felles nøkkel for fortsatt å kunne sende hemmelige meldinger til hverandre. Fordelen med symmetrisk kryptering er at de matematiske metodene som benyttes, gjør at kryptering av store tekstmengder kan utføres raskt.

5.4 Asymmetrisk kryptografi

Håndterer problemet med distribusjon av nøkler. Hver deltaker har i utveksling av hemmelige dokumenter to ulike nøkler - et nøkkelpar. En av nøklene er hemmelig og bare kjent for eieren. Denne kalles den private nøkkelen. Den andre nøkkelen vil være offentlig kjent og tilgjengelig for alle andre deltakere. Denne nøkkelen kalles den offentlige nøkkelen. Den matematiske metoden som ligger til grunn, gjør det mulig å benytte den offentlige nøkkelen til å kryptere en meddelelse slik at bare den private

[18] kilde: http://odin.dep.no/

nøkkelen kan dekryptere den. Ulempen med denne måten å kryptere på er at den er tidkrevende ved kryptering av store tekstmengder.

Asymmetrisk kryptografi har flere muligheter enn bare kryptering av dokumenter. Dersom man krypterer en meddelelse med den private nøkkelen, er det bare den offentlige nøkkelen som kan dekryptere den. Dette ga opphavet til digitale signaturer.

Publisering

Systemet fungerer slik at den eller de som ønsker å publisere en ny fil, sender nettverket en innleggingsmelding (insert) som omfatter filen og dens utpekte lokaliseringsuavhengighet globale unike identifiserings nøkkel (GUID), Den får da tildelt en GUID som medfører at filen blir lagret på flere noder, (hvis den er over 1MB i størrelse) en del av filen kan bli lagt på en node i Norge mens resten av filen kan havne i USA eller Kina, man vet rett og slett ikke hvor den legger seg. Under en fils levetid kan den flytte seg til andre noder eller bli erstattet av en nyere versjon, for å motta en fil må brukeren foreta en forespørsel som inneholder (GUID) nøkkel, når forespørselen får kontakt med en annen node, det behøver ikke å være den første noden man treffer på hvor filen er lagret, tar denne noden og sender dataen tilbake til den noden som sendte forespørselen.

GUID Nøkler

Freenet GUID nøkler er kalkulerte til å bruke SHA-1 sikkerhets hashes (nøkkeltransformasjon). Nettverket bruker to hovedtyper nøkkeltransformasjon (hashes) den ene er CHK (Content-hash key)(innhold nøkkeltransformasjon), brukt primært til lagring
Og den andre er SSK (Signed-subspace key)(signert-underordnet rom nøkkel) som ment til bruk for høynivå. Disse to er vesentlig for noder og filnavn i et konvensjonelt fil system.

7.1 CHK (Innhold-nøkkeltransformasjon)

CHK nøkkelen er en lav nivå data lagrings nøkkel som er generert med nøkkeltransformasjon av innholdet i filen som skal lagres. Denne prosessen gir hver fil en unik identitet som kan bli verifisert veldig hurtig. I motsetning til url adresser i www, så kan du være sikker på at CHK referansen vil peke til den eksakte lokaliseringen av filen. CHK tillater også kopier av den samme filen lagt inn av forskjellige personer, på grunn av at systemet vil kalkulere den samme nøkkel for denne filen.

7.2 SSK (Signert-underordnet-rom nøkkel)

SSK setter opp et personlig navneområde (plass) som alle kan lese, men bare eieren av denne plassen kan skrive til. Du kan for eksempel lage et navneområde med et bestemt emne som eks: et særemne som du ønsker å skrive om, med å først generere en tilfeldig offentlig-privat nøkkel parvis til å identifisere dette emne. For å legge til en fil så må du først velge en kort tekst beskrivelse av dette emne eks: emne/særemne/politisk-papirer. Du må deretter kalkulere filens SSK nøkkel med å hashe den offentlige delen av SSK og deretter beskrive tekst innholdet før du samkjører dem og hasher dem på nytt. Signering av den private delen av SSK nøkkelen medfører at en integritets sjekk blir gjort for hver node som behandler en signert-underorndet-rom fil som verifiserer dens signatur før den aksepterer denne.

For å motta en fil fra Freenet. Trenger du bare SSK nøkkelen, som kanskje er lagret på din nøkkel ring allerede og deretter å skrive inn tekstemne

Routing

Routing forespørsler er det mest viktige med hele Freenets systemet.

8.1 Napsters måte

Den simpleste routing metoden, brukes av fildelingssystem som Napster, er å vedlikeholde en sentral indeks for filer. Sånn at brukerne kan sende en forespørsel direkte til informasjons kilde. Uheldigvis skaper sentralisering en veldig lett måte å angripe systemet på. For eksempel: hvis du prøver å få tak i telefonnummeret til en kjent person, den enkleste måten for å gjøre dette vil ordinert ha vært å ta kontakt med et telefonselskap eller søke i gule sider/telefonkatalogen, men fordi disse tjenestene er sentralisert så kan din forespørsel om dette bli blokkert hvis den kjente presonen har valgt å ikke være oppført i dette systemet (Hemmelig nr.), eller hvis noen har valgt å fjerne denne personen fra dett systemet.

8.2 Gnutellas måte

Systemer som Gnutnella sender sine forespørsler til hver enkelt node i systemet i en hvis radius. Ved å bruke denne metoden så vil du spørre alle dine ”venner” om noen av dem vet tlf.nr. til den kjente presonen, for igjen å få dem til å spørre sine venner osv.
Innen kort tid vil tusenvis av personer lete etter dette tlf.nr. Selv om denne prosessen vil til slutt greie å finne tlf.nr så er det bortkastet tid og uakseptabelt bruk av ressursene.

8.3 Freenets måte

Freenet unngår begge disse problemene ved å bruke SAHCS (steepest-ascent hill-climbing serch) (Spisstårn-stigning bakke-klatring søk): Hver node sender spørringen til noden den tror er nærmest kilden. Du kan starte søket etter den kjente presonen ved å spørre en venn som har jobbet sammen med denne kjente presonen som sender beskjeden vider til en som i dag jobber sammen med denne kjente presonen som igjen gir beskjed til den kjente presonen som da tar kontakt med deg. På samme måte funger Freenet opp mot nodene, de nodene som er nærmest kilden blir kontaktet og videreformidler kontakten videre til den noden som har de kilde opplysningene som du forespør.

Søke etter publiseringer på Freenet?

Freenet er ikke søkbar på den tradisjonelle måten som vi ellers er vant med, slik som Internett.
Nettverket er fundamentalt annerledes enn begge klientserver modellene som brukes på www, de har rett og slett ikke faste sentral servere i sitt system, hele systemet deres bygger på noder slik som Fast Track og Gnutnella (og andre peer2peer systemer), dette er en konsekvens av Freenets konsept for anonymitet.

9.1 Hvordan søke

Siden nodene ikke vet hva som er lagret på deres krypterte datastore, så vil de ikke ha noen ide om det matcher med en søke tekststreng som for eksempel: musikk filer mp3. hvis du foretar en spørring. Dette beskytter deg med å gi deg en troverdig benektelse og at du ikke er ansvarlig for innhold som er ulovlig/straffbart, og at du ikke selv vite hva som ligger lagret på din datamaskin. Dette henger sammen med at måten Freenet lagrer ting på gjør at dataene blir spredt over hele verden og at det ikke er noen som kan bevises at det er du som har forespurt eller lagt inn disse dataene/filene, eller andre for den del.

9.2 Freesites

Det nærmeste du kan komme i sammenligning med søkemotorene på www er at i Freenet er det noe som heter freesites som har linker til andre freesites i form av nøkler som peker mot andre ting og steder. I noen tilfeller disse er funnet med edderkopper, som er et program som ”krabber” (søker) i nettverket med å følge alle linkene du finner og katalogiserer resultatet, dette er det samme som www søkemotoren til Google gjør. FIND er en sånn edderkoppskapt portal som er det som skaper kontakt mellom to enheter og bruker en standard web brukergrensesnitt som startside. Nye sider kan bli lagt til via NIM (Nearly Instant Message) i noen tilfeller, eller det kan bli lansert på Frost freesite-annonse bord (med andre ord en oppslags tavle for linker, lik ABC startsiden).

Freenet applikasjonsprogrammer

Hvis du kjører noen Freenet applikasjoner som ”frost” eller ”fmb”, så kan systemet bli mye treger når det gjelder surfing på Freenet.

10.1 Hva er Frost

Frost er en slags elektronisk nyhets melding og fildelings program som brukes i Freenet. Fildeling i anførselstegn siden det ikke virker i et normalt peer2peer system men kun i Freenet.

10.2 Frost

Data kan også bli oppdaget og søkt etter på din egen maskin å bli funnet der. Dette er hvordan filene blir funnet av frost eller hvordan dette programmet jobber seg frem. Et ny installert frost vil returnere få nøkler selv om du søker etter * (alt), men over tid vil antall filer som den vet om øke etter hvert som den ser flere opplastnings meldinger. Noen kan lage nye applikasjonsprogrammer som gjør noe lignende for å søke Freesites lokalt, men pr i dag er det ikke virkelig nok til å gjøre dette verdt kontra det å bruke edderkopp-genererte indekser.

Sikkerhet

Freenet tilbyr ikke ekte anonymitet slik som andre systemer eks: Mixmasters og Cyperpunk remailers gjør. Det meste av sporingen som disse systemene er designet til å parere.
I Freenet vil denne type sporing kunne bli ”lett” å bruke for noen som har til hensikt å identifisere noen som foretar en forespørsel etter noe på Freenet. Men vel å merke de kan kun spore til den første noden. Altså kun den personen som foretar spørringen og frem til den første noden han treffer på, deretter er det umulig å spore videre. Det vil også være vanskelig å bevise at det er denne personen som har foretatt spørringen da det kan være andre som har forespurt via denne personens node.

11.1 Den første noden

Uansett hva du gjør på freenet så vil din identitet være relatert til den første noden som du kontakter eller kommer i kontakt med, selv om du begrenser deg selv til kun å snakke med noder/personer som du kjenner/ har tillit til må de være nødt til å snakke med resten av nettverket på et eller annet tidspunkt. Anonymiteten som freenet tilbyr er bare en uklar måte å tilby anonymitet på, på grunn av at det er vanskelig å bevise at det er du eller din node som ikke har sendt en forespørsel, eller innlegging av data på vegne av andre eller om det er noen andre som har gjort det.

11.2 Problemet

Problemet er at den eneste måten du kan gi ekte anonymitet til dine klienter, er at klientene selv kan direkte kontrollere routingen av data, om må derfor kryptere data med en serie av nøkler av nodene som dataene vil passere (ala mixmasters). Freenets dynamiske routing kan ikke tilby dette. Så for å opprettholde virkelig anonymitet så må du sende data gjennom et eksternt nettverk av anonyme remailers.
I Freenet er det programvaren som gjennom dynamisk routing som velger hvilken node du skal kontakte, du kan ikke velge selv.

11.3 Angrep

Freenet er designet til å være et effektiv og dynamisk lagringssystem. Hvis informasjonen er forespurt mange ganger fra en mengde av noder så vil nodene som forespør gå via lagringssystemet og lagre informasjonen, dette for å holde nede mengden av data på nettverket. Hvis informasjon blir innlagt på et begrenset sett av noder og deretter tidvis forespurt fra en separat node, med repetisjon, vil oppsettet lukkes en etter en i nettverkt til den nærmeste node og den opprinnelige noden blir lidende for angrepet.

Med andre ord for å skade freenet systemet med et angrep av typen overfylling, så må du hele tiden skifte innfallsvinkel for å komme deg inn i nettverket og kontinuerlig sette inn/legge inn eller forespørre ny data, og du vil fortsatt bare øke arbeidsmengden i nettverket som er linjert med ditt eget. Gitt at en uendelig kapasitet større enn det totale innhold av hele nettverket. Så er det mulig å invalidisere/ødelegge et hvert offentlig nettverk (til og med Internett) med overfylling. Men det er deres intensjon å alltid holde freenet så motstandsdyktig som det teoretisk er mulig.
Så med andre ord systemet er ikke så sårbart for overfylling av data, som er en metode som angriperne vanlig vis bruker for å fylle opp lagringskapasiteten til et system for å sette det ut av sin virksomhet.

11.4 Sensur

Det samme hvis noen prøver å sensurere en fil/data/dokument så er det pga. krypteringen og lagringsplasseringen av data, vil det i systemet ikke være mulig å lokalisere dataene til et bestemt fast eller geografisk sted.

11.5 Infiltrering

Eksistensen av en ondskapsfull node[19] innen et nettverk er den største utfordringen og det vanskeligste problem som et distribuert nettverk står overfor. Det har vært banen for mange tidligere systemer før. Mange systemer prøver å unngå ondskapsfulle noder med å holde tilgangsprotokollen[20] stengt. Men de har fortsatt ikke sett et eksempel på at ondskapsfulle noder virker i det lange løp. Uansett strider dette mot freenets filosofi. Freenet er basert på en balanse av positive og negative tilbakemeldings løkker som bringer forespørsler for informasjon til en node når dens fungerer bra, og utelater forespørslene fra noden hvis den ikke fungerer bra. Nøkkelen for å unngå infiltrering er å sikre disse løkkene til å identifisere til og med den mest utspekulerte og ondskapsfulle noden som er skapt til infiltrering av systemet og å ikke sende forespørsler til den. Dette spørsmålet er ikke fult avklart med den nåværende test koden, men du kan være sikker på at det er mange mulige løsninger. Dette temaet har lenge vært oppe til diskusjon men er enda ikke helt avklart.

11.6 Nye typer angrep

Freenet prøver hele tiden å oppdatere seg på nye typer angrep, det er pr. i dag ingen som har klart å infiltrere eller angripe systemet deres på en effektiv måte[21]. De oppfordrer derfor folk til å prøve hvis de ønsker, for å gjøre systemet enda bedre i følge dem selv. Det må nevnes at det er ikke noen nettverk som er prefekt og kan tilby det alle måtte ønske

11.7 Juridisk omgåelse

Hvorfor brukes hash nøkler og kryptering av data i noden/brukeren egen datastore (harddisk)? Dette er gjort for å unngå at eieren av noden ikke skal kunne bli straffet. Det er jo ikke meningen at node eier skal vite hva som ligger lagret i datastoren på sin egen maskin, men det er jo bare for han eller henne hvis det er ønskelig å forespørre de data

---

[19] Ondskapsfull node/cancer node er en maskin der bruker har til hensikt å skade nettverket/systemet eller å ødelegge for de andre i systemet i form av virus, flooding, hacking og andre ting som kan forstyrre eller ødelegge for andre i et system.

[20] Protokoll: oppføring av for eksempel ip, mack adresse for å tillate eller å blokkere personer adgang til et bestemt sted eller område i nettverket.

[21] Kilde: http://www.freenetproject.org/

som ligger i sin egen datastore for å finne ut hva som ligger lagret der, på samme måte som det andre gjør når de forespør data.
Men man kan jo heller ikke forvente at de som er eiere av noden med dens datastore skal greie å gjette seg til nøkkelen til data/filene som ligger lagret på maskinen.
Systemet er laget slik for at det skal være mulig å juridisk unngå å bli straffeforfulgt for lagringen av data på grunn av det teknisk aspekt.
Det handler derfor mer om det juridiske enn det tekniske i måten dette gjøres på.

Hva med Overgrepsbilder og Terrorisme?

Freenet sier ”at selv om mesteparten av menneskene ønsker at overgrepsbilder og terrorisme ikke fantes. Så skulle menneskeheten ikke prøve å forhindre disse menneskene fra deres frihet til å kommunisere, da det er et fåtall av mennesker som ønsker å benytte seg av denne friheten.”[22]. Dette er noe som vi ikke kan være enige med Freenet i da vi ikke er villige til å tillate mennesker med slike hensikter å lagre slikt materiale på våres datamaskiner.

12.1 Hva om jeg ikke vil at min maskin/node skal brukes til å lagre slikt materiale

Freenet sier ”den sanne testen om noen ønsker å tro på ytringsfrihet er om de tolererer at andre har meninger som de selv ikke er enige i eller om de finner slikt materiale frastøtende eller motbydelig. Hvis du ikke ønsker at slikt materiale skal bli lagret på din node så oppfordrer freenet deg til å ikke bruke Freenet[23].”
Vi mener at den sanne testen på ytringsfrihet er at folk kan si sin mening, uten at det skal ha noen konsekvenser for hva de sier.
Men at man skal ikke kunne dekke deg bak ytringsfriheten for å begå ikke moralske overgrep, trakassering eller i så måte fysiske overgrep for å oppnå eller utføre kriminelle handlinger. Eller være nødt til å måtte lagre materiale som man finner frastøtende eller motbydelig.
Vi vil derfor oppfordre alle til å følge Freenets eksempel hvis man er uenige i deres fortolkning av ”Den sanne testen”

[22] Kilde: www.freenetpoject.org
[23] Kilde: www.freenetpoject.org

Positive sider med Freenet

13.1 Anonymitet:

Det som kan sies å være positivt med Freenet er at hvis du ønsker at ingen skal vite hvem du er og hva du foretar deg på nett så tilbyr de et ganske godt anonymt ståsted for deg i din utforsking, i motsetning til Internett der du er helt åpen og ute i det offentlige rom uten at du selv egentlig behøver å være klar over det. Dette gjelder også i særlig grad andre typer fildelingsprogram som ikke tilbyr den samme anonymitet som det freenet gjør.

13.2 Sporing

Det er også veldig lett for eventuelle myndigheter eller andre som er nysgjerrige på hva du gjør på nett å spore deg, og kartlegge eventuelt hva du foretar deg og hva du måtte ha liggende av annet materiale på din maskin.
Man har i Freenet heller ingen myndigheter overordnede eller andre overvåknings organer som sitter og sensurerer det du ønsker å lese, debattere eller publisere noe som forekommer hyppig i medier som ligger på Internett og andre fildelingssystem.

13.3 Verktøy

Freenet tilbyr også dette som et verktøy til mennesker uten fri meningsflyt i land hvor de for eksempel: er politisk undertrykte eller andre land hvor myndighetene slår hardt ned på mennesker som taler i mot systemet. Eller har meninger eller lyster som ikke er tolererbart i forhold til det samfunnet de kommer fra måtte akseptere.

13.4 Markedskreftene

Du blir heller ikke utsatt for reklame, popups eller skreddersydd reklame rettet mot den enkelte bruker slik som du blir i den vanlige delen av Internett/fildelings systemer. Altså ikke utsatt for kommersielt press fra markedskreftene.

13.5 Andre brukere

For folk som er psykisk syke[24] eller folk som ikke vil legge igjen elektroniske spor etter seg, kan nok dette være et godt verktøy for disse gruppene, da Internett er et område der alle kan, hvis de vil, se hvem eller hva som blir gjort, altså et område som folk med slike

[24] Paranoia, forfølgelsesvanvidd og tidligere forfulgte eller undertrykte personer pga. politiske meninger etc.

problemer ikke regner som sikkert. Slik at ”de” også kan benytte seg av dataalderens finneser på lik linje med andre brukere. Freenet sier jo at alle typer mennesker med dårlige eller gode intensjoner kan benytte seg av deres medium[25].

13.6 Økonomi

For mennesker med dårlig økonomi kan dette verktøyet bidra til at de kan foreta nedlastinger av materiale som man ellers måtte betale mye penger for.

13.7 Intensjonen

Hvis, og bare hvis, at intensjonen til utviklerne av freenet hadde blitt brukt til hva det i utgangspunktet ble planlagt til så hadde hele freenet konseptet kunne sies å være positivt, noe som dessverre ikke blir fulgt.

Negative sider med Freenet

14.1 Brukerterskel

Systemet kan sies å være negativt i forhold til at du må ha forholdsvis gode it-kunnskaper for å i hele tatt kunne installere og bruke systemet, det er altså ikke forbeholdt alle å kunne bruke dette, da oppsettet av programvaren er ganske komplisert og bruken likeså.

14.2 Tregt

Det er også et veldig ressurskrevende og tregt system grunnet all kryptering og nøkkel indekser og at systemet er under stadig utvikling noe som gjør at det ikke hele tiden er de beste løsningene som blir brukt, men at de prøver ut forskjellige måter å få systemet til å fungere bedre på, før de endelig tar i bruk det som virker best.

14.3 Hastighet

Det kan også redusere din hastighet på nettet at du må dele bandwith med resten av brukerne og det kan gå lang tid å finne de data du måtte finne på å forespørre da systemet må krabbe gjennom alle nodene for å finne akkurat denne forespørselen.

[25] Kilde: www.freenetpoject.org

14.4 Tilgjengelighet

Det samme må sies om at dataene ikke er tilgjengelig til en hver tid da det ikke er noen permanente lagringsenheter som er koblet på til en hver tid, da noden som inneholder den data du ønsker kan bli avslått midt under nedlastingen.

14.5 Søkemuligheter

Det er heller ingen muligheter til å søke etter data slik som i www, (du skriver inn en tekst i søkemotorene på Internett.) du er nødt til å forespørre nøkler som du på forhånd vet hvilken data denne nøkkelen måtte inneholde. Noe som er svært tungvindt for brukere som er vant til å søk etter informasjonen på www.

14.6 Dårlige intensjoner

Mennesker med dårlige hensikter slik som for eksempel: Nazister, terrorister, pedofile og andre kriminelle vil også kunne bruke freenet uten å bli fanget opp av rettsystemer.
Dette har ført til at folk med slike hensikter som nevnt over har en plass eller ”Fristed” der de kan treffe likesinnede, der de får tilgang til materiale som er av deres interesse, som de kanskje ellers ville ha store problemer med få tilgang til.
Dette medfører også at de får et større nedslagsfelt og at de kan bygge opp en større omgangskrets med likesinnede, noe som kan føre til at ”problemet” kan vokse.
Uten at myndighetene har mulighet til å kunne spore opp eller sette en stopper for slike aktiviteter.

14.7 Bekjempelse

Negativt i forhold politiets/myndighetene arbeide med å avverge og bekjempe terrorist komplott og andre kriminelle handlinger som overgrepsbilder og eventuelt organisert kriminalitet, er at det enda ikke foreligger noen god måte å overvåke systemet og at man i liten eller ingen grad kan spore personer med slike hensikter i dette systemet.

14.8 Omgåelse av lovverk

Måten systemet omgår det juridiske lovverket på med kryptering, slik at personer kan nekte en hver befatning med data som ligger lagret på sine respektive maskiner og det er heller ingen kontroll mulighet for å si at det er denne personen eller andre for så vidt som har forespurt disse data.

14.9 Kontroll over egen maskin

Den enkelte bruker har heller ingen mulighet til å se hva som måtte finnes av materiale som er lagret i sin egen maskin (”datastore”). Noe som igjen kan føre til at eieren av maskinen kan få lagret store mengder med uønsket data på sin maskin. Og pr. i dag er det ikke kriminelt i forhold til konseptet, men ved lovendring slik at systemet ikke kan omgå lovverket kan du bli straffet for de data som er lagret på maskinen din.

14.10 Liten mulighet til nedlasting av store datamengder

Liten mulighet til å laste ned/opp filmer, spill og annet materiale som inneholder store data mengder i Freenet, noe som er lett i andre fildelings systemer, og på grunn av kryptering og dekryptering av slikt materiale er dette en utrolig ressurs og tid krevende prosses i Freenet.
Systemet til Freenet gjør det fult mulig å laste ned slike data mengder, og har du god tid er det jo da ikke noe problem, men som nevnt tidligere, vil dette gå utrolig tregt og bruke lang tid.

Konklusjon - Er Freenet mulig å bruke som distribusjonskanal for Overgrepsbilder

Kan Freenet brukes til å laste opp/ned overgrepsbilder:
Svaret er ubetinget JA (hastigheten på større filer er riktig nok en begrensende faktor). Det vil være fult mulig å distribuere og laste ned overgrepsbilder uten at noen som helst kan sensurere eller overvåke handlingen på bakgrunn av Freenets anonyme, oppsplittede og krypterte system. Det vil fungere dårlig hvis det dreier seg om filmer eller andre typer som er av større mengde data, da dette er en veldig stor prosses og en særdeles tidkrevende operasjon på grunn av krypteringen og hastigheten. Mens bilder og andre publikasjoner som ikke inneholder store datamengder ikke er noe problem. Det vil heller ikke være noen mulighet, slik vi ser det for politiet å spore vedkommende som forespør eller publiserer dette materialet på bakgrunn av systemets oppbygning og virkemåte.

Muligheter for politiet å spore overgreps bilder i dette nettet

16.1 I liten grad

Vi tviler sterkt på at det er noen isp'er (Internett service provider) som greier å se noe av den krypterte trafikken. Politiet kan gå inn på Freenet og eventuelt se hva som finnes og omfang men de har ingen mulighet til å spore hvor dette/det ligger direkte. Det er selvsagt mulig å spore ip-adressen der du laster det ned fra, men den personen du da sporer har ingen anelse om hva som ligger i hans datastore, vi er ikke sikker på om hvordan dette vil slå ut rent juridisk. De kan også spore ip-adresse til den første noden de treffer på men der etter er det stopp, de vil ikke ha noen mulighet til å spore videre fra denne noden eller forespørselen som går til de andre nodene som blir forespurt videre fra den første noden etter slikt materiale og likeledes er jo heller ikke disse nodene klar over hva som måtte befinne seg av data i sin datastore.

16.2 Infiltratører

Det kan være en mulighet for politiet å benytte seg av infiltratører men lovligheten av dette vet vi ikke noe om. Der infiltratøren setter opp en egen node som etter lang tid kan bli en såkalt "trusted node" og bruker denne til å komme i kontakt med grupperinger som innehar og besitter slikt materiale via chat (prate) kanaler i Freenet, det er jo en stor sannsynlighet for at disse grupperingene sitter med nøkler til slikt materiale som de deler bare seg i mellom i stede for å publisere dette over hele Freenet sitt nett. Da kan det være en mulighet for politiet å greie å få tak i navn og ikke bare nick (kallenavn) for å få identifisere vedkommende.

16.3 Canser noder (Kreft noder)

Det vil også være utrolig ressurs krevende for politiet å kunne sette opp såkalte canser noder (kreft noder) for å floode (overfylle) Freenet og likeledes har Freenet tenkt på denne muligheten til å angripe deres system, men i teorien skal dette kunne fungere, om det juridiske aspektet av dette er lovlig er lite sannsynlig.

16.4 Nye metoder

Det er i midlertidig dukket opp et nytt system når det gjelder sporing som enda er på forsøkstadiet men det virker lovende i slikt henseende. Systemet baserer seg på sporing av hardware noe som ikke kan manipulerest med slik som ip-adresser og mac-adresser kan manipulerest. Vi tror at dette kan bidra til at politiet kan greie å knekke systemet (de greier å se hvem som publiserer og forespør slikt materiale) til Freenet med denne metoden, i nær fremtid, hvis de får tilgang til dette nye systemet, og at det fri stilles ressurser til å bruke dette systemet, når det foreligger klart til bruk.

For å beskrive denne nye metoden siterer vi fra Win.XP.no:[26]

”Føler du deg trygg på at du har skjult din aktivitet på Internet bak smarte "gardiner"? Ikke vær for sikker på det. En forsker ved University of California sier han har funnet en måte å identifisere datamaskinvare på. Denne teknikken kan for eksempel brukes til å avsløre anonyme nettsurfere gjennom å forbigå noen vanlige sikkerhets-teknikker.”

”Tadayoshi Kohno, en doktorgrads-student, skriver dette om sin forskning: -"Det er nå flere kraftfulle teknikker for å ta fjernstyrte "fingeravtrykk" av operasjons-systemer, det vil si å spore disse på Internet. Vi har nå puffet disse ideene enda lenger, ved å introdusere en metode til å spore opp og ta "fingeravtrykk" av fysisk hardware, uten å trenge dette utstyrets samarbeid i prosessen".

”Potensialet for Kohto's teknikk er enormt vidtrekkende. For eksempel kan det være mulig å spore fysisk utstyr når det koples til Internett fra flere forskjellige punkt, herunder også et utstyr bak et NAT, uansett om dette utstyret bruker fast eller tilfeldig IP-adresse. Dette omfatter også fjern søk og sporing av blokker av adresser for å bestemme om adressene korresponderer med virtuelle verter.”

”NAT, eller network adress translation, er en protokoll som er vanlig å bruke for å la det se ut som maskiner bak en brannvegg har samme IP-adresse på Internett.”

”Kohno og hans team har testet sine teknikker på mange forskjellige operasjons-systemer, inkludert Windows XP og 2000, Mac OS X Panther, Red Hat og Debian Linux, FreeBSD, OpenBSD, og også Windows for Pocket PC 2002.”

Kanskje ikke lurt å føle seg fullt så trygg på total anonymitet på Freenet fremover, allikevel!

[26] Kilde: http://www.win-xp.no/
Kilde: c|net News.com.com

Avslutning

Det er jo positivt at mennesker uten fri meningsflyt har et medium til å kunne uttale seg. Men slik som Freenet er pr i dag, så kan det jo bli et fristed og en yngleplass for pedofile og andre avvikere, slik at de kan opprettholde sine syke interesser ved å benytte seg av dette systemet.
Vi har ikke selv undersøk i Freenet om det er blitt slik i dag, men ut i fra kildene[27]og det vi har lest om dette materialet, kan det jo virke som om at det allerede er blitt slik.
Det vi ser nå er nesten det samme som vi har sett når det gjelder den organiserte kriminaliteten som har spredd seg som en kreftbyll i den vestlige delen av verden, de med dårlige intensjoner får en mulighet til å bli med i internasjonale grupper av likesinnede, mot at de før hadde en begrenset geografisk nedslagsfelt og mulighet til å finne likesinnede, og at de i dag har hele verden som boltreplass.

Freenet vil jo også i fremtiden bli en plass der folk med dårlige intensjoner vil tiltrekkes da Internett er i ferd med å bli en plass som avslører slike.

Freenet konseptet har slik vi ser det startet en fristed med å tillate, i sin streben etter full ytringsfrihet at folk med såkalte dårlige intensjoner som terrorister, pedofile og andre kriminelle som får fri tilgang til denne type medier for å kunne utfolde seg fritt uten fare for å bli sensurert eller på noen annen måte straffeforfulgt for sine handlinger. Dette er slik som vi ser det helt forkastelig, da vi ikke er enig med Freenets måte å tenke på. Vi er ikke villig til å opprettholde en slik type/medium for at disse aktørene skal kunne boltre seg uhemmet.
Ytringsfriheten er en menneskerett i et hvert demokratisk samfunn men det må jo ikke være for enhver pris at man skal opprettholde den, det er jo tross alt fremtiden til våre barn det er snakk om. Skal de måtte vokse opp i en verden der pedofile og terrorister skal kunne utfolde seg fritt uten at det skal få noen konsekvenser for dem.?

Vi er ikke enige i Freenet s måte å argumentere for ytringsfrihet da dette vil føre til at vi tillater at personer med uetiske hensikter å lagre ulovlig materiale slikt som overgrepsbilder på våres eller andres maskiner.
Vi vil også si at disse umoralske personene som lagrer eller erverver seg slikt materiale enten det er de eller andre som har gjort det, så må jo det på et eller annet tidspunkt ha skjedd et fysisk overgrep, og da er det ikke rett at de kan gå ustraffet fra dette!

At Freenet dekker seg bak ytringsfriheten til undertrykte og politisk forfulgte mennesker for å virkeliggjøre sine visjoner der alt skal være tillatt. Blir galt når man tenker på alle som kanskje er ødelagt for livet som en konsekvens av dette, det være seg terrorisme, narkotika, overgrepsbilder og andre kriminelle handlinger. Dette er rett og slett moralsk forkastelig.

[27] : http://www.openp2p.com/pub/a/p2p/2000/11/21/freenetcontent.html

Når det gjelder målsettingen til Freenets utviklere så er den slått heller dårlig til, da det er blitt et medium der hele 88% av brukerne[28] er fra den rike vestlige verden mens den fattige undertrykte verden som de egentlig hadde som målsetting å bli et verktøy for, er bruken så liten at den ikke er målbar. Så vidt vi kan se har ikke Freenet organisasjonen dokumentert noe som kan vise til at dette er blitt et verktøy for dem det var tenkt til.

Når det gjelder det økonomiske aspektet til Freenet så skal det jo være et non profitt selskap så hva er egentlig drivkraften? Så det kan jo ikke i følge dem være kapitalismen. Om intensjonen til idealistene bak Freenet var å skape et verktøy eller en mulighet for dem til å ligge et skritt fremfor myndighetene eller bare en genuin interesse er vanskelig å avgjøre, men vi heller til å tro at det er muligheten for dem til å ligge et skritt fremfor myndighetene heller enn å lage et verktøy som er drivkraften bak Freenet.

Den eneste måten politiet kan ha muligheter til å slå ned på dette er at det i budsjettet til justisdepartementet settes av mer penger til å utdanne folk og innkjøp av tekniske virkemidler slik at de som jobber med dette problemet kan bli oppdatert på lik linje med de som utfører disse kriminelle handlingen. Altså flere resurser.

Hvis ikke man er villig til å starte en 3 verdenskrig som utspiller seg i cyberspace der alle landene prøver å angripe slike systemer eller overfylle disse med data som er ubrukelig for de med dårlige intensjoner. Og dermed gjøre systemene ubrukelig for alle ved å bruke flooding. Det er slik vi ser det den eneste måten å virkelig bekjempe dette problemet på.

Man kan godt si at Freenet gjenspeiler deler av vårt samfunn. På den ene siden sitter myndighetene og prøver å forhindre kriminelle komplott og eller overgrep av diverse slag noe som de lykkes med til en hvis grad, men når det gjelder elektronisk overvåkning så mangler de resurser etter det vi har fått opplyst. Og på den andre siden sitter de som er kritiske til myndighetenes overvåknings politikk, datatilsynet og andre som ønsker å ivareta personvernet til den enkelte. Det må jo ikke bli slik at vi skal blir en politistat, der alt du gjør skal kunne overvåkes eller sensureres av våre myndigheter på bakgrunn av at andre misbruker ytringsfriheten! Noe som skjer i Freenet.

[28] http://www.itic.ca/DIC/News/2004/05/freenet_TOP10_countries.jpg

Kilder

http://itpro.no
http://freenet.sourceforge.net/
http://www.sv.uio.no/
http://jtcfrost.sourceforge.net/
http://www.lights.com/
http://wikiserver.freenethelp.org
http://detritus.net/
http://www.skypoint.com/
http://www.infoanarchy.org/
http://nightwatch.mine.nu/
http://www.lawtechjournal.com/
http://www.ddj.com/
http://www.digi.no/
http://www.openp2p.com
http://www.win-xp.no/
http://www.freenetproject.org/
http://odin.dep.no
http://www.itic.ca/DIC/News/2004/05/freenet_TOP10_countries.jpg
http://www.openp2p.com/pub/a/p2p/2000/11/21/freenetcontent.html
http://www.freenetproject.org/papers/freenet-ieee.pdf
http://www.supremecourtus.gov/
http://www.epic.org/
http://www.google.com/search?hl=no&q=Human+Rights+Watch%2BInternett&lr
http://www.gilc.org/
http://hrw.org/advocacy/internet/
http://www.savepacifica.net/20020126_schubb.html
http://www.ominous-valve.com/pac/archive/020125starr_imc.html
http://conferences.oreillynet.com/cs/p2pweb2001/view/e_spkr/563
http://www.math.chalmers.se/~ossa/
http://www.nyu.edu/pages/linguistics/courses/v610003/shan.html
http://www.digi.no/digi98.nsf/pub/dd20011008120323__10325474
http://java.sun.com/j2se/1.4.2/docs/api/org/w3c/dom/Node.html

Proxyer

Anonym på Internett?

Gruppearbeid utført av:

Kjell-Magne Kristiansen
Einar Selnes
Kenneth Nerdal
Eva Daabach
Unni Pedersen
Ronny Pedersen

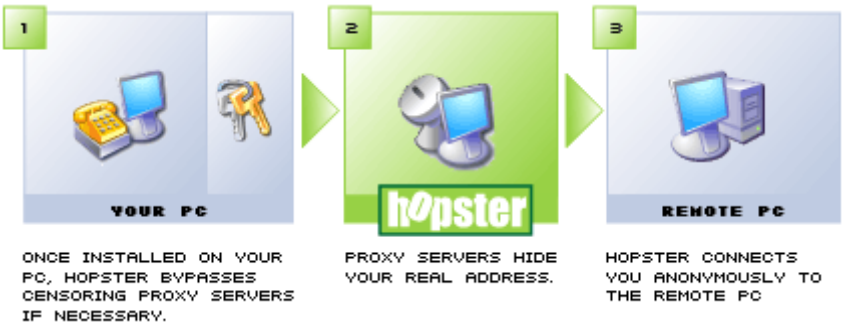
Samfunnsinformatikk IN 116

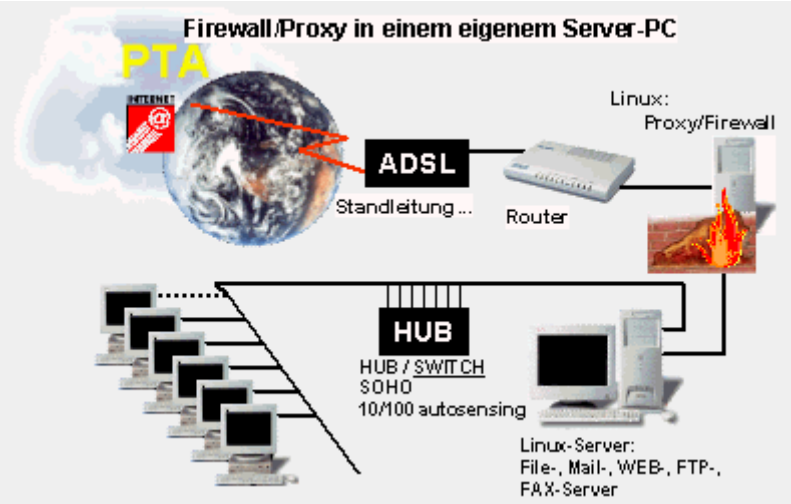
Informasjonsteknologistudiet

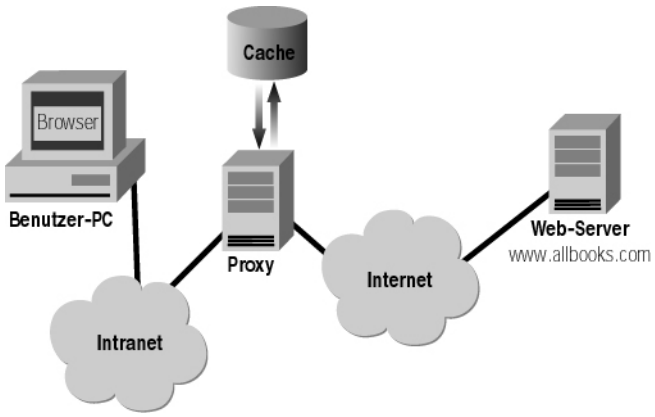
ved

Høgskolen i Nesna, avdeling Mo i Rana

Vår 2005


1
YOUR PC
2
hopster
3
REMOTE PC
ONCE INSTALLED ON YOUR PC, HOPSTER BYPASSES CENSORING PROXY SERVERS IF NECESSARY.
PROXY SERVERS HIDE YOUR REAL ADDRESS.
HOPSTER CONNECTS YOU ANONYMOUSLY TO THE REMOTE PC


Firewall/Proxy in einem eigenem Server-PC
PTA
Linux:
Proxy/Firewall
ADSL
Standleitung ...
Router
HUB
HUB / SWITCH
SOHO
10/100 autosensing
Linux-Server:
File-, Mail-, WEB-, FTP-,
FAX-Server


Cache
Browser
Benutzer-PC
Proxy
Intranet
Internet
Web-Server
www.allbooks.com

Innledning

Dette er resultatet av en gruppeoppgave i Samfunnsinformatikk våren 2005. Vi hadde valget mellom to oppgaver og vår gruppe valgte den oppgaven som gikk ut på å sette seg inn i hva en Proxy er og hvordan disse fungerer .
Hovedfokuset i oppgaven skulle være mot såkalte anonyme Proxyer og ikke Transparente (åpne) som kun er satt opp for å regulere Internettrafikken.
Vi skulle innenfor den tidsfristen som var satt, finne så mange Proxyer som mulig og hvem som sto som ansvarlige for disse.
De ansvarlige skulle kontaktes og vi skulle be om en logg over aktiviteter på de vi hadde valgt ut.
Dersom vi fikk tilbakemeldinger på våre henvendelser, skulle vi gå igjennom loggen(e) og analysere bruken av dem.
Spørsmålene vi skulle vurdere var:

1. Kan noe tyde på at trafikken kan relateres til overgrepsbilder?
2. Lastes det opp og ned bilder og filmer?

Siste del av oppgaven går ut på å konkludere og begrunne denne, med hva vi har funnet i løpet av den tiden vi har hatt til disposisjon.

Proxyer

For å forstå hva en Proxy er og hvorfor den brukes, må vi først enkelt forklare hvordan Internett brukes. En klientmaskin sender en forespørsel til en tjenermaskin. Denne sender det forespurte innholdet tilbake til klienten.

Hvordan kjenner så tjeneren igjen klienten? Ved og bruke domenenavn og IP- adresse. Domenenavn er unikt og en måte å kjenne igjen og lokalisere datamaskiner og kilder knyttet til Internett. Enhver som ønsker å ha en nettside/sted, må registrere seg med et domenenavn som brukes til online-identitet, et navn som kunder og internettbrukerne må bruke for å få adgang til de tjenester f.eks. en nettside eller e-post skal utføre. Høgskolen i Nesna har domenenavnet hinesna.no og interesserte kan sende e-post til nn@hinesna.no. Et godt domenenavn er lettere å huske, og kampen om gode domenenavn er stor, da det i dag er registrert mer enn 11 millioner domenenavn i hele verden. Det finnes flere nettsted som tilbyr hjelp med dette.

Hvert domenenavn er knyttet til en numerisk IP(Internett Protokoll) adresse. Den består av sett med 4 siffer, hver mellom 0 og 255 og delt i perioder. Internett bruker IP-adressen for å kunne sende data. Domenenavn systemet (DNS) er en samling databaser med informasjon om domenenavn og dets IP adresser og har som oppgave å koble disse sammen. Disse to må være unike da det ellers fører til full forvirring når en IP adresse må gjenkjennes i forhold til sin eier. F. eks dersom høgskolene i Bodø og Nesna hadde samme domenenavn. Mer om dette finner du på www.isc.org, hjemmesida til Internett Systems Consortium og /eller www.whois.net (what is domainname).

Hva er en Proxy?

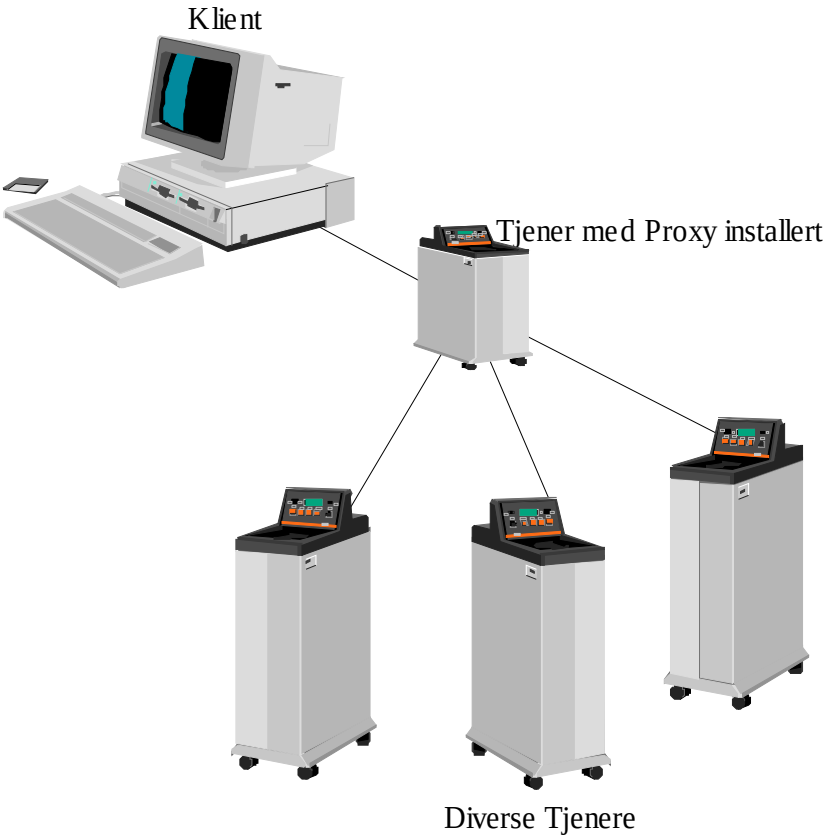
En Proxy er et program på en PC/tjeneren som er tilknyttet en spesiell port på PC- en hvor den er installert.

En Proxy er software som i utgangspunktet var ment for å utføre sikkerhetstjenester samt andre funksjoner som web- og innholdscaching. Vanligvis så settes en Proxy opp på en multihomed PC, det vil si en PC med to nettverkskort, det ene med tilgang til Internett og det andre til ditt interne LAN (Local Area Network).

Et godt ord for en Proxy er mellomledd.

> Et eksempel:
> Du sitter internt på jobben og ønsker å lese en webside på Internett. Men jobbnettet er konfigurert slik at det ikke er mulig å kommunisere direkte med den webtjeneren du egentlig vil kommunisere med. Derimot er du i stand til å kommunisere gjennom en Proxy som befinner seg internt i jobbnettet et sted. Den kan både kommunisere med deg og tjenesten på Internett.

Et viktig konsept med Proxyer er at de håndterer spørringer på vegne av klienter på et nettverk.



Klienten sender en forespørsel til en tjener med installert Proxy som skjuler klientens IP-adresse og videresender forespørselen med sin egen IP-adresse.
Den tar så imot svar på forespørselen og sender dette tilbake til klienten.

Når en PC på et nettverk spør etter en fil fra Internett gjennom en tjener hvor det er installert en Proxy, det være seg en nettside, filer, bilder eller tilsvarende, tar Proxyen over og oversetter spørringen for så å sende den videre med Proxyens offentlige IP-adresse. På denne måten vil det se ut som at opphavet til spørringen er Proxyen.

Anonyme Proxyer.

Alle Proxyer som ”gjemmer” en klients IP-adresse blir kalt anonyme Proxyer.

Det finnes flere typer Proxyer med forskjellig grad av anonymitet.
Fire av de mest brukte er HTTP Proxy, SOCKS 4 / SOCKS 5, CGI Proxy og FTP Proxy.

HTTP Proxy (Hyper Text Transfer Protocol)

Dette er den mest brukte Proxyen. Hvis man hører ordet Proxy, så betyr det en HTTP Proxy.
Ved hjelp av denne typen Proxy er det mulig å vise en webside, se på bilder og laste ned filer.
Nyere versjoner av programmer som ICQ etc. kan også brukes gjennom en Proxy.
Den tillater arbeid over Internett med HTTP og noen ganger FTP. Den kan også cache (mellomlagre), informasjon lastet ned fra Internett.

Det er mulig å lage seg lenker av Proxyer for å gjøre seg mer anonym, men man trenger spesielle program for dette. Det går også an å lage seg virtuelle tunneler gjennom en administrativ Proxy.

Du kan også laste ned e-post i Outlook som en anonym bruker.

SOCKS Proxy

Sammenlignet med HTTP Proxy er SOCKS en veldig ny Proxy og det finnes to typer SOCKS:
SOCKS 4 som arbeider med TCP- protokoller (Transmission Control Protocol)
SOCKS 5 som arbeider med TCP- protokoller og UDP- protokoller (User Datagram Protocol)
En SOCKS Proxy overfører simpelthen data fra en klient til en tjener uten å trenge gjennom til innholdet i dataene. Derfor kan den arbeide med HTTP, FTP, SMTP etc.
Den utgir seg for å være klienten da den ikke sender med noen slags form for informasjon om seg selv til webtjeneren. Den har bare et anonymitetsnivå og det er veldig høyt.
Den mest brukte er versjon 4, men den nyere versjonen støtter veldig mange av de populære programmene som ICQ, Napster, Audio Galaxy etc.
Kan settes opp i lenker for å høyne anonymiteten enda bedre, men trenger programvare for dette.
Kan også brukes for å hente e-post, men må da ha spesielle program.

CGI Proxy (Web Proxy / Anonymizer)

En CGI Proxy representeres som regel som en webside. Veldig lik sidene for søkemotorer, men i stedet for å skrive inn søkeord, så skriver man inn URL til de sidene man ønsker å se. URL som man går til, er ikke skrevet i adresselinjen, men det kommer fram som en falsk URL for at ingen skal kjenne igjen sidene man har vært inne på. Ved bruk av en slik Proxy kan man surfe anonymt uten å forandre på innstillinger i browseren og uten å installere tilleggsprogrammer.
CGI Proxy støtter HTTP, HTTPS og noen ganger FTP. Kan lett settes opp i lenker for å høyne anonymiteten. Er dessverre veldig vanskelig å hente e-post fra e-postprogrammer.

Ulikt andre typer Proxyer har CGI Proxyen bedre mulighet for å filtrere informasjon.
Den hindrer kjøring av aktivt innhold (Java Script etc.) i en webside og hindrer utsendelse av cookies til en klient.
Krypterer URL til den adressen man forespør slik at hvis man f. eks. sender en forespørsel til www.yahoo.com gjennom en CGI Proxy så vil man se noe som ligner på dette i adresselinjen: http://www.cgi-Proxy.com/abcd104dlsjuywe34sdfispd345klksfdsl Systemadministrator som sjekker loggen til tjeneren, vil da ikke kunne finne ut hvilken tjener man har vært hos (www.sex.com eller www.altavista.com).

Både HTTP og CGI Proxyer har fire konvensjonelle anonymitetsnivå:

1. **Transparent** - Ikke anonym. Lar webtjeneren se at det er en Proxy som er i bruk og gir fra seg IP-adressen til klienten. Bruken av en slik Proxy er informasjonscaching og/eller støtte for internett-tilgang for flere PC- er via en enkel tilkobling.
2. **Anonymous** - Lar webtjeneren se at det er en Proxy som er i bruk og gir ikke fra seg IP-adressen til klienten.
3. **Distorting** - Lar webtjeneren se at det er en Proxy som er i bruk og gir fra seg en falsk IP-adresse til klienten som blir generert tilfeldig.
4. **High anonymous** (elite) - Lar ikke webtjeneren se at det er en Proxy som er i bruk og gir heller ikke fra seg IP-adressen til klienten. Web-tjeneren tror at den jobber direkte mot klienten.

FTP Proxy (File Transfer Protocol)

Denne typen Proxy er spesialisert og tilegnet arbeid bare med FTP tjenere. Man kan bruke disse Proxyene i de mest populære filprogrammer (FAR. Windows Commander, etc.), nedlastningsprogrammer (CuteFTP, GetRight, etc.) og i browsere.

Tabell for egenskaper til 3 proxytyper

Egenskaper	HTTP	SOCKS	CGI
Støtter protokoll	HTTP, FTP (Av og til)	HTTP, FTP, POP3, SMTP, UDP, alle TCP / IP	HTTP, FTP (Av og til)
Støtter Proxy-lenker	Av og til (trenger SSL støtte)	Ja	Ja
Trenger programvare	Browser med Proxy-støtte	Spesielle program for å arbeide med SOCKS	Bare browser
Enkel i bruk	Du må vite hvordan man setter opp en Proxy i en browser	Du må kjenne til disse spesielle programmene og hvordan disse skal settes opp	Kjennskap til bruk av internett
Anonymitet	Transparent, anonym, høy anonymitet	Kun høy anonymitet	Transparent, anonym, høy anonymitet
Vanskeligheter ved å lage Proxy-lenker	Veldig vanskelig (Du trenger spesielle program)	Vanskelig (Du trenger spesielle program)	Enkelt (Du trenger ikke å forandre noen innstillinger)
”Gå bak ryggen på” en administrativ Proxy	Vanskelig	Bare hvis den administrative Proxyen er en SOCKS	Veldig lett
Tilleggstrafikk for bannere	Nei	Nei	Ja (Av og til veldig mye)

39

[39] http://www.freeproxy.ru/en/free_proxy/faq/proxies_comparsion_table-htm

Er det mulig å surfe helt anonymt via en Proxy?

Hvorfor være anonym? Ikke i utgangspunktet for å delta i ulovligheter, men for å beskytte personlig informasjon og hindre at den kommer i hendene på markedsførere som sender deg bannerannonser samt redusere mengden av søppelpost.

Når du surfer på Internett så legger du igjen veldig mye informasjon om deg selv:
- Navn og versjon av browseren
- Navn og versjon av operativsystemet
- Konfigurasjonen av browseren (skjermoppløsning, fargedybde, Java / JavaScript-støtte, etc.)
- IP-adressen på klienten
- Annen informasjon

Den viktigste delen av denne informasjonen og absolutt nødvendig for en webtjener er IP-adressen. Ved å bruke IP-adressen kan man finne ut følgende om klienten:
- Hvilket land den er i.
- Hvilken by den er i.
- Leverandørens navn og e-post.
- Din fysiske adresse.

Alt som sendes fra en klient til en tjener kalles variabler, og hvis informasjon ikke blir sendt til en tjener, forblir variablene tomme.

Dette er noen av variablene:
REMOTE_ADDR - IP-adressen til en klient
HTTP_VIA - Hvis den ikke er tom, så blir en Proxy brukt. Verdien er adressen (eller flere adresser) til en Proxy tjener. Disse variablene blir lagt til av Proxyen, hvis du bruker en.
HTTP_X_FORWARDED_FOR – Hvis den ikke er tom så blir en Proxy brukt. Verdien er en reell IP-adresse til en klient. Denne variabelen blir også lagt til av Proxy tjeneren hvis du bruker en.
HTTP_ACCEPT_LANGUAGE - Hvilket språk som er brukt i en browser (Hvilket språk en side burde vært vist i).
HTTP_USER_AGENT – Såkalt ”a user’s agent”.
HTTP_HOST – er en web-tjeners navn

Dette er bare en liten del av variablene som finnes, og noen eksempler på verdiene av variablene:
REMOTE_ADDR – 194.85.1.1
HTTP_VIA – 194.85.1.1 (Squid/2.4.STABLE7)
HTTP_X_FORWARDED_FOR – 194.115.5.5
HTTP_ACCEPT_LANGUAGE – ru
HTTP_USER_AGENT – Mozilla/4.0(kompatibel; MSIE 5.0; Windows 98)
HTTP_HOST – www.webserver.ru

Variabler som vises ved bruk av Proxyer

Anonymiteten ved bruk av Internett er bestemt ut fra hvilke variabler som er ”gjemt” for webtjeneren. Som tidligere nevnt er alle Proxyer som ”gjemmer” en klients IP-adresse blir kalt anonyme Proxyer.

Hvis en Proxy tjener ikke er i bruk så vises disse verdiene:
REMOTE_ADDR – Klientens IP-adresse
HTTP_VIA – Ikke fastsatt
HTTP_X_FORWARDED_FOR – Ikke fastsatt

Hvis man bruker en ”Transparent Proxy”:
REMOTE_ADDR – Proxyens IP-adresse
HTTP_VIA – Proxyens IP-adresse
HTTP_X_FORWARDED_FOR – Klientens IP-adresse

Hvis man bruker ”Simple Anonymous Proxies”:
REMOTE_ADDR – Proxyens IP-adresse
HTTP_VIA - Proxyens IP-adresse
HTTP_X_FORWARDED_FOR - Proxyens IP-adresse
Blant alle de andre Proxyene er ”Simple Anonymous Proxies” den mest brukte.

Hvis man bruker ”Distorting Proxies”:
REMOTE_ADDR – Proxyens IP-adresse
HTTP_VIA - Proxyens IP-adresse
HTTP_X_FORWARDED_FOR - Tilfeldig IP-adresse

Hvis man bruker ”High Anonymity Proxies (Elite proxies)”:
REMOTE_ADDR – Proxyens IP-adresse
HTTP_VIA – Ikke fastsatt
HTTP_X_FORWARDED_FOR - Ikke fastsatt

Dette betyr at verdien på variablene er det samme som om en Proxy ikke er i bruk, med unntaket av en veldig viktig ting – Proxyens IP-adresse blir brukt i stedet for klientens IP-adresse.
Uansett om klienten bruker en transparent eller en anonym Proxy, så er det kun IP-adressen som holdes skjult. All annen informasjon kan være tilgjengelig (Konfigurasjonen av browseren slik som skjermoppløsning, fargedybde, Java / JavaScript- støtte, etc.)[40]

[40] http://www.symantec.no
http://www.freeproxy.ru/free-proxy/faq/proxy-anonymity.htm og http://www.stayinvisibel.com
http://www.anonymizer.com

Er det mulig å spore klientens IP-adresse bak en anonym Proxy.

Det finnes anonyme Proxyer som kan brukes for å surfe anonymt på Internett. Det er også interessant å være klar over at det finnes mange måter for å spore en klient bak en anonym Proxy:

Cookies

Dette er små informasjonskapsler som sendes mellom webtjener og klient. Den blir lagret i klientens browser for å bli hentet av webtjeneren ved neste forespørsel til samme tjener. Metoden blir da som følger: Klienten sender en forespørsel via en Proxy til en webtjener. Tjeneren sender tilbake en cookie som inneholder Proxyens IP-adresse, sammen med siden klienten har forespurt. Ved neste forespørsel til samme adresse ser webtjeneren etter om klienten har en kjent cookie, men denne gangen inneholder cookien klientens reelle IP-adresse. Tjeneren konkluderer da med at det er en annen som forespør adressen.

JavaScript / VBScript

Det finnes spesielle underprogram (scripts) som kjøres av klientens browser. Uansett hvor mye man prøver å sette opp browseren så har man ikke mulighet til å gjemme sin reelle IP-adresse. Disse scriptene er klassifisert som veldig enkle program med veldig få funksjoner, men de sporer klientens IP-adresse like godt som å spore mange av innstillingene på browseren. Disse scriptene kan forandre innstillingene på browseren også. Den beste måten for å beskytte klientens browser er å totalt forby kjøring av slike script.

Java

I motsetning til JavaScript, er Java et eget programmeringsspråk. Java-programmer er dyktigere til å spore IP-adressen og forandre browserens innstillinger. Å beskytte klientens IP-adresse fra å bli sporet av Java-programmer er mye mer komplisert. Den sikreste måten å gjøre det på er å umuliggjøre kjøring av Java, men siden Java har mange nettverksfunksjoner så blir det vanskelig å koble dem alle ut.

ActiveX / Plug-ins

Er forskjellige tilleggsfunksjoner på browseren. Disse funksjonene er i realiteten særegne programmer som kjøres på klienten. De har en bredere kapasitet enn Java og JavaScript og kan lettere oppdage innstillingene på browseren og spore klientens reelle IP-adresse. De kan også med letthet forandre innstillinger på Proxyen.

Med andre ord så er det mulig å sikre klientens IP-adresse med flere metoder:

- Koble ut cookies
- Koble ut diverse scripts
- Koble ut Java
- Koble ut ActiveX

Men hvis man kobler ut alle disse funksjonene, så vil det i praksis si at man får vanskeligheter med å fram noe som helst fra webtjenere.

Kontakt mot Proxyeiere og diverse nyhetsdiskusjonsfora.

Ved å bruke diverse nettsted med søkemotorer som kunne gi informasjon om anonyme og andre Proxyer, fant vi eierne til de IP- adressene vi valgte ut samt de opplysninger som lå registrert på dem. (Se vedlegg nr 1).Vi sendte først e-post til ca. 40 Proxyeiere med en forklaring om at vi hadde som oppgave å finne ut hva Proxyer ble brukt til og om de vennligst kunne sende et loggeksempel. Vi fikk ingen logger utlevert.
Vi fikk endel svar, men de aller fleste av de som leverte tilbakemelding var automatiske svar som forklarte hvorfor de ikke kunne utlevere loggene til oss, og svar om at adressen ikke fantes eller et autosvar med takk for varsling av søppelpost og virus (bugs) etc. I tillegg fikk vi svar om at de ikke ville gi ut loggen da kundene hadde valgt dem for å kunne være anonyme.

Men ved ett tilfelle sendte vi til en Proxy som var rangert som høy anonymitet, og fikk tilbakemelding fra en systemansvarlig om at de ikke hadde en Proxy, (se eks: e-posten vi sendte og tilbakemeldingen vi fikk).

Da IP - adressen ikke førte til samme informasjon for systemansvarlig som den gjorde for oss, er det høyst sannsynlig at IP - adressens levetid hadde gått ut og var tatt i bruk av en annen Proxytjener.
En annen mulighet er at denne eieren ville forbli anonym, eller så var det reelt at de ikke hadde kjennskap til at det var en kjørende Proxytjener på deres nettverk

Noen av tilbakemeldingene vi fikk viser at leverandører av Proxytjenester setter anonymiteten til brukerne høyt. Andre innehavere av Proxyer var oppsatt med sikkerhetsrutiner for beskyttelse mot søppelpost og virusangrep.

Eks: på Sendt e-post

Dette er e-posten som ble sendt ut til alle vi har kontaktet. Der lover vi at evt. Logger skal anonymiseres.

To whom it may concern.

08.03.2005

We are a group of computer students from Nesna University College.
We are doing an assignment in Sosial Informatics on the topic of Proxy Servers, specifically the various ways people use this service.
As a part of our assignment we need to analyze the log files of a random group of Proxy Servers, we are not interested in the IP addresses from the users.
We would be very obliged if you kindly could send us a log/history from your Proxy Server for a period of one or two days. All results will be anonymous and there will be no reference to your Proxy in our final report.
We hope you can help us.
If you need more information you can contact
Associate Professor Per A. Godejord at e-e-post: pag@hinesna.no
The web page of Social Informatics is here:

http://it-mo.hinesna.no/~pag/pag/engelsk.html

Yours sincerely

Kenneth Nerdal

Student group Alpha

Dep. of Computer Science
Nesna University College, Norway

Utdrag av noen domenenavn og Proxyer som det er sendt e-post til:

Domenenavn	Opplysninger	Land	IP adresse	Hvor anonym
Nerim.net		Frankrike	80.65.229.73	Anonym
Esat.net	IENET	Dublin, Irland	193.120.73.239	Anonym
Comcast.net	Comcast Cable Comm	USA	68.38.122.103	Anonym
Yahoo.com	Gharegazloo	Teheran, Iran	80.191.68.194	Anonym
Egynet.com.eg	Mourad	Egypt	62.139.54.218	Anonym
Griffin.net/ Griffin.com	GIS-MB-LCC Commun.	England	83.148.145.89	Anonym
Nic.ad.jp	Chiyouda-ku	Tokyo, Japan	219.163.100.195	Anonym
We-dare.nl		Nederland	217.148.184. 7	Anonym
Tiscali.com.de		Tyskland	212.255.122.105	Høy anonymitet
Telefonidca.es		Spania	80.25.156.238	Anonym
NIc.br	CBG comite Gester da	Brasil	200.140.131.194	Anonym
Ita.tip.net/ Ilsole240re.it		Italia	212.45.97.9	Anonym
Telefonica.es		Spania	217.125.31.160	Anonym
Ripe.net	LJP5-RIPE	Israel	212.143.159.190	Anonym
Sunrise.net	Netvision.net	Sveits	194.158.247.154	Anonym
Interbusiness.it/ Telecomitalia.it	Institutotecnico Industrialestat	Italia	82.191.190.66	Anonym
Mtn.co.za		Sør-Afrika	196.11.239.37	Høy anonymitet
Publicf.bta.net.cn		Kina	61.135.158.102	Anonym

Eksempel på hvilke opplysninger vi fikk på søk via whois.net

80.65.229.73
Record Type:
IP Address

OrgName: RIPE Network Coordination Centre
OrgID: RIPE
Address: P.O. Box 10096
City: Amsterdam
StateProv:
PostalCode: 1001EB
Country: NL

ReferralServer: whois://whois.ripe.net:43

NetRange: 80.0.0.0 - 80.255.255.255
CIDR: 80.0.0.0/8
NetName: 80-RIPE
NetHandle: NET-80-0-0-0-1
Parent:
NetType: Allocated to RIPE NCC
NameServer: NS-PRI.RIPE.NET
NameServer: NS3.NIC.FR
NameServer: SUNIC.SUNET.SE
NameServer: AUTH62.NS.UU.NET
NameServer: SEC1.APNIC.NET
NameServer: SEC3.APNIC.NET
NameServer: TINNIE.ARIN.NET
Comment: These addresses have been further assigned to users in
Comment: the RIPE NCC region. Contact information can be found in
Comment: the RIPE database at http://www.ripe.net/whois
RegDate:
Updated: 2004-03-16

Eksempel på mottatte svar på sendt E-post

Av hensyn til at til at vi lovte at evt. svar som skulle brukes i oppgavene skulle anonymiseres, er navn, domenenavn og IP er skrevet med ****.

Svar nummer 1:

Re: Proxy server assignment

Date: Wed, 9 Mar 2005 10:08:10 +0100

Hi!

I'm sorry but we don't have any Proxy servers.

Regards

Dette var den første tilbakemeldingen. Vi sjekket på nytt IP - adressen og fikk opp samme resultat. Vi skrev så nytt brev til adressen vi fikk opp og fikk svar tilbake. under viser vi e-posten vi sendte med påfølgende svar.

We have used a website to search for Proxy servers, and got information from using whois on the following IP address ***.**.***.* The result told us that your behind a Proxy server.
The reason that I reply to this e-post is to inform you, that on your system there are a running High Anonym Proxy server. And if you find it, could you be so kind to shear the log with us of the Proxy.
Tank you for taking the time to write to us.

Svar nummer 2:

Hi!

The IP address ***.**.***.* is not ours... The IP addresses that ******* ********* ** uses are ***.**.***.**, ***.**.***.* to ***.**.***.*** and ***.**.***.* to ***.**.***.***

According to RIPE (www.ripe.net) ***.**.***.* belongs to "addVise Inredning ********** **"
http://www.ripe.net/fcgi-bin/whois?form_type=simple&full_query_string=&searchtext=***.**.***.*

Regards

Første eksempel på automatisk tilbakemelding:

Re: Proxy server assignment

Date: Wed, 9 Mar 2005 05:39:06 +1000

****
(This is an automatic response - please do not reply to this message)
****

Hello

Your e-post to <****@****.**> has not been delivered.

The hostmaster e-postbox is designed specifically for requests
from ***** account holders. E-posts that do not conform to the
designated account holder's format are not delivered to
******@****.**.

No other ***** e-postboxes are filtered in this way, so please
read the information below about how to resend your e-post.

Instructions for resending your e-post

Non ***** account holders - use a different ***** e-postbox

If you are not a member or an account holder, *****
maintains a number of e-postboxes for you to use. A list of
***** e-post addresses is located at:

http://www.****

If you want to report spam or network abuse, please read
the FAQ "Reporting network abuse: spamming and hacking" at:

http://www.****

***** account holders - resend with account name in subject

All e-post to the hostmaster e-postbox must include a valid
account name in the subject line. The account name must
be enclosed in square brackets or parentheses.

EXAMPLES:

Correct: Subject: [EXAMP-ID]
or
Subject: (EXAMP-ID)

Incorrect: Subject: {EXAMP-ID}
or
Subject: EXAMP-ID

Please note that your account name is not the same as the actual name of your organisation. Account names are assigned by ***** when applications are processed and are follow the format:

XXXXX-YY

Where: XXXXX - based on the name of the member
YY - country code

If you are unsure of your exact account name, please contact:

Please resend your original e-post to ******@***.***, this time including your account name in the subject line.

THIS IS AN AUTOMATED RESPONSE

Please note, replies to this message will NOT be read. If this e-post has not provided the information you need, please refer to other ***** contact addresses, which are described at:

Andre eksempel på automatiske tilbakemeldinger:

We will NOT handle this message: [Proxy server assignment]

Date: Tue, 08 Mar 2005 20:07:24 +0100 (CET)
Fra: MESSAGE REJECTED[+]
Til: gruppealpha@student.hinesna.no[+]

****
* Your e-e-post will NOT be sent to a **** *** Hostmaster *
****

The message:

has been received at the **** ***.

The **** *** Automatic Hostmaster Robot has extracted the following additional information:

RegID: No valid RegIDs found
Ticket Numbers: No ticket number in e-post

It is of type NOREGIDBOUNCE.

We were unable to determine the originating Local Internet Registry (LIR) for this request. If the request is originating from an LIR, please re-submit, adding the RegID in the related field within the request form or in the body or the header of the message as specified below:

x-ncc-regid: <Reg_ID>

For information on how we decide to process and prioritise requests please see:

http://www.******.**

Or send a e-post with the subject ROBOTHELP to *****@****.**.

Eksempel på at Proxyeier ivaretar anonymitet.

1. eksempel

Re: Proxify - - -

Dato: Sat, 26 Feb 2005 10:09:08 -0500
Fra: *****
Til: Gruppealpha[+]

[Kilde] [Vis meldingshode]

Proxify is strongly committed to protecting the privacy of its users.
We will not reveal any information about our users or their surfing
habits to you.

2. eksempel

RE: assignment Proxyservers

Dato: Thu, 24 Feb 2005 13:22:35 +0100

Dear Kenneth,

I forwarded your e-post internally.
Unfortunately are the responsible not willing to give these data.
I have therefore regretfully to decline your request.

PGP key-ID 0x0FBF6D7D

Privileged/Confidential Information may be contained in this message. If you are not the addressee indicated in this message (or responsible for delivery of the message to such person), you may not copy or deliver this message to anyone. In such case, you should destroy this message and kindly notify the sender by reply E-e-post. Please advise immediately if you or your employer does not consent to Internet E-e-post for messages of this kind. Opinions, conclusions and other information in this message that do not relate to the official business of my firm shall be understood as neither given nor endorsed by it.

Eksempel på sikkerhetsrutiner

Please confirm your message

Dato: Sat, 26 Feb 2005 10:04:22 -0500 (EST)

<< IMPORTANT INFORMATION REGARDING YOUR MESSAGE TO ****@***.**** >>

Due to the tremendous amount of spam, viruses, and worms currently circulating via e-e-post, we have found it necessary to protect our business e-e-post system with a confirmation process that verifies incoming correspondence as legitimate.

Confirmation of your e-e-post address with the **** Abuse Desk is a one-time process per sending e-e-post address. Once you have confirmed (by simply replying to this e-e-post) all future correspondence you send to ***** Abuse Desk from your confirmed e-e-post address will be given priority treatment. If in the future you choose to contact us from a different e-e-post address, you will need to go through the process again for that new address.

To confirm that you did send the message below, simply reply to this e-e-post, sending back the contents of this message. You do not need to add or edit anything.

If you did not send the e-e-post below, it is possible that your e-e-post address was forged by a spammer; in order to hide their identity, spammers will often randomly select an e-e-post address from their lists and insert it in the "From" and/or "Reply To" fields. If so, you can safely ignore this message and may disregard the confirmation process described above.

We appreciate your cooperation.

***** Internet Investigations and Security Services Team
For your reference, the original e-e-post you sent is attached below.

Gjennomgang av det materialet vi fant.

Da våre e-posthenvendelser til Proxyeierne ikke har gitt oss de loggene vi var ute etter, måtte vi finne andre måter å jobbe på.

Ved å bruke søkemotoren Google er det gjennom f.eks. siden til www.whois.net, mulig å lete på nettdomener og IP-adresser. Det er da mulig å få enkelte treff på denne måten, selv om det er angivelig Proxyer som skal være anonyme. Antall treff varierte mye og mange var aktivitetslogger til nettsider samt at det var svært mange logger som angikk virus- og søppelpost trafikk.
F.eks. vi fant en nettside som et tilbud til homofile arabere samt homofile og dating. I tillegg en sexside med e-postadresser for iranere, ei nettside som tilbyr hjelp til å lage undergrunnsfilmer og ei side for frie ytringer for folk i Egypt.

Den andre måten vi kunne få opplysninger var via fora som diskuterte bruk av Proxy. Et par av gruppemedlemmene gikk inn på disse med fiktive navn

Drøfting

Ved å kun plukke tilfeldige IP - adresser og domenenavn og sende e-post, så er sjansen for å treffe på Proxyer som brukes til ulovligheter, rimelig liten. De sidene vi har brukt for å finne fram til anonyme Proxyer har på 100 - vis med lister over Proxyer (Se vedlegg. Skal man virkelig finne noe, må absolutt alle tilgjengelige domener og IP - adresser gjennomgåes. Et veldig omfattende arbeid se f.eks. www.ISC.org om survey. Deres surveytjeneste bruker flere dager når de gjennomgår alt, og vi snakker om over 1 milliard domenenavn og IP - adresser. Selv om det i prinsippet er mulig å finne fram til brukere og eiere av IP -adresser som skjules via en Proxy, er arbeidet tidkrevende og faren for at enkelte skifter IP-adresser eller at Proxyen legges ned (kort levetid), rimelig stor.

Hovedinntrykket hittil i arbeidet vårt, er at de fleste bruker anonyme Proxyer til lovlige aktiviteter. De funnene vi har til nå greid å spore opp, omhandler nettsider som formidler sex, porno, homofili og ytringsfrihet i land med sensur.
Vi er kjent med at det rundt omkring i verden er forskjeller i synet og lovligheten av f.eks. homofili. Nettsidene som omhandler bl.a. homofile arabere, og homofili generelt, retter seg mot personer som bor i land hvor dette er enten forbudt eller det fortsatt ikke er full åpenhet rundt dette temaet. Det er derfor forståelig at de vil bruke anonyme Proxyer,
for å kunne spre sitt budskap og/eller ha et forum de kan benytte seg av for å uttrykke det de føler.

Nettstedet som vi fant i forbindelse med en anonym Proxy brukt i Iran, er også et uttrykk for at de som ønsker å snakke om og/eller skaffe seg en sexpartner i et slikt forum, må bruke en anonym Proxy. Å praktisere dette er ikke mulig på en åpen måte i et ultraislamittisk land som Iran fortsatt er.
Spørsmålet videre er om materiale med overgrepsbildergrafisk innhold kan lastes ned via slike sider. Flere av sidene opererer med krav til medlemskap dersom man skal ta seg videre

inn på det materialet/aktivitetene som befinner seg på nettstedene. Ved at man forlanger brukernavn og passord, er det grunn til å stille spørsmål.
Forståelsen for at brukere vil være anonyme er grei og at nettsideeieren ønsker en viss kontroll på bruken. Men kan sidene brukes til ulovlig aktivitet? Vi kan stille spørsmålet, men ikke gi noe konkret svar. Muligheten for å skjule slikt er til stede, men det vil også være mulig på andre nettsider som krever medlemskap og hvor innholdet er av en mer allsidig karakter. Jfr. en av sidene som vi fant i forbindelse med en oppgave vi har hatt tidligere. Der lå det alminnelige opplysninger i tillegg til oppskrifter på eksplosiver og porno.

Definisjonen av en Undergrunnsfilm kan være så mye. Det er grunn til å anta at også filmer med overgrepsbildergrafisk innhold vil kunne bli produsert og distribuert via en nettside for folk som ønsker å lage filmer som har et innhold som ikke blir sensurert i en offentlig sammenheng. Nettstedet var såpass nytt at ikke alle detaljer kom fram på nettsiden. Det kan derfor være grunn til å følge litt med på hva som skjer på de sidene i en tid framover.

Etter å ha lest på forskjellige diskusjonsfora, sitter vi igjen med en formening om at det ikke er mulig å skjule IP-adressen gjennom en anonym Proxy. Proxyer er en usikker måte fordi man vet ikke hundre prosent sikkert om det ikke blir ført en logg av aktiviteter på denne og at andre kan derigjennom enkelt spore tilbake til klienten dersom noen får tak i loggen. Det mange glemmer er at leverandøren fører logg over filer som går inn og ut fra klientens Internettilkobling. La oss si at en Proxy er i Brasil, og all trafikk som blir sendt fra Proxyen til klienten blir logget hos den lokale leverandøren til klienten. I dette tilfellet er anonymiteten ikke til stede. Proxyen til den eventuelle IP-adressen forandres hver gang man kobler seg på, men det er bare de to siste tallene. Dermed er det ingen stor sak å finne det aktuelle IP-adressen på en Proxy-logg.
Problemet ligger da i å få tak i rett logg. Hvis for eksempel Nye Kripos ber om en logg, kan det nok forekomme at det er en ”pyntet” logg som blir presentert, og det vil være dårlig reklame med en logg som viser til websider med tvilsomt innhold.

Det er ikke alle tjeneradministratorer som er kjent med at det er satt opp Proxy på deres tjener. I disse tilfellene blir det selvfølgelig vanskelig å legge ansvaret på enkeltpersoner.
Det finnes programmer som gir deg muligheten til å surfe anonymt på nettet (eks. Anonymizer 2004). Disse programmene gjemmer IP-adressen din og krypterer surfingen med ”Surfing Security™” 128bit kryptering. (128bit er visst ikke en helt sikker kryptering, da det også finnes krypteringsverktøy som kan knekke koden).

Skriver man ”hidden ip” i søkeboksen til Google, finner man linker til forskjellige fora som diskuterer forskjellige måter å ”gjemme” seg på nettet ved å bruke Proxy. Bakdelen med disse programmene er at de er ”uferdige”. Det vil si at de gjør maskinen treg etter en tids bruk. Disse programmene vil sannsynligvis bli bedre slik at de blir mer interessant å bruke.

Det er også steder på nettet hvor man blir identifisert via IP-adressen og som kan stenge ute brukere på grunn av nasjonalitet eller usømmelig oppførsel med mer. Et godt eksempel på dette er prateprogrammet Mirc.

Mirc har mange pratekanaler med forskjellige temaer, f.eks. kan kanalen Finland tillate bare personer med finsk IP-adresse. I dette tilfellet er det også personer som tar i bruk Proxyer for å forandre IP-adressen så det er mulig å få tilgang til kanaler som de av forskjellige grunner ikke har tilgang til.

Det viser seg at noen pratekanaler ikke tolererer noe snakk om overgrepsbilder. Om det er fordi de er totalt imot dette eller om det ligger noe ”snusk” bak kanalen, kan vi bare spekulere i.

Enkelte av gruppemedlemmene gikk inn på noen kanaler og spurte ganske direkte på dette med overgrepsbildergrafi. De ble bedt om å fjerne seg, noe som kan vise at de ikke vil ha brukere som etterspør dette.

Nye Kripos har gått inn i en avtale med flere ISP-er (Internet Service Provider) om filtrering av Websider der overgrepsbilder og andre overgrepbilder blir vist. Men med hjelp av en eliteproxy, har folk muligheter til å unngå disse filtrene. Man kan m.a.o. omgå sin egen ISP og de begrensninger som er lagt inn.[•]

[•] Kilder: http: //www.samair.ru/proxy/proxy-06.html/

Sammendrag/konklusjon:

Første del av oppgaven gikk ut på å finne ut om Proxyer og hva kan de brukes til. Det er ikke vanskelig å finne stoff om dette emnet på nettet. Enten så kunne vi bruke rene opplysningssider, eller så var det mer enn nok stoff i forbindelse med nettsider med leverandører som selger proxysoftware. Disse anbefaler sine produkter og spesielt anonyme Proxyer bl.a for at du unngår at andre ser/følger med på hva du gjør samt at skal slippe å bli neddynget av søppelpost, reklamer o.s.v.

Som den andre delen av oppgaven skulle vi prøve å få tak i logger på bruken av Proxyer via Proxyeierne. Der oppnådde vi ikke det vi var ute etter, noe som virket litt frustrerende til å begynne med, men vi fant jo fort ut at det hadde sin forklaring i at de ville ivareta sine kunder.

Vår erfaring basert på svarposten vi fikk, er at de som er eiere av Proxyer ikke vil gi ut logger som vil identifiserer brukerne som har benyttet deres Proxyer. Det er jo i tråd med at anonyme Proxyer har til hensikt å skjule brukerens identitet og IP-adresse.
Mange benytter seg derfor av anonyme Proxyer i den tro at de da er "usynlige" på nettet.

Etter å ha lest på forskjellige fora om hva anonyme Proxyer er og hva de brukes, sitter vi igjen med en formening om at det ikke er mulig å skjule IP-adressene. Anonyme Proxyer er derfor ikke en sikker måte å være anonym på, fordi det kan bli ført aktivitetslogger og ISP –eiere kan følge med på trafikken på sine linjer, bredbånd og kan spore seg tilbake til bruker/klient.

Sist men ikke minst viktig med oppgaven var å finne ut om anonyme Proxyer kunne bidra til at enkelte brukere kunne bruke disse til å laste ned eller sende innhold med overgrepsbilder/overgrepsbildergrafi.
Vårt arbeid viser at mange bruker anonyme Proxyer for å holde identiteten sin skjult bl.a. fordi en god del av dem p.g.a at de ikke liker å bli overvåket. På de foraene vi var innom, forteller mange at bruker anonyme Proxyer til helt vanlig surfing. Og gjennom Googletreffene ser vi at de som bor i land hvor det er sensur på f.eks homofil må benytte seg av en anonym Proxy for å unngå å bli straffet. Det er vel ikke tvil om at dette kan brukes for surfing og nedlasting av overgrepsbildergrafi. Så lenge folk tror de er uten identitet, så tar mange sjansen på å bruke Internett mer ”åpent”
De fleste brukerne setter seg ikke inn i alt om hva Proxyer er og vil derfor tro på det leverandøren har lovet angående anonymitet. De som er ute etter overgrepsbilder o.l vil derfor se det mulig å uten hindringer laste ned og videresende innhold med overgrepsbildergrafi.

Spørsmålet videre er om anonyme Proxyer vil kunne velte NyeKripos og Telenors satsning for bekjempelse av kriminelle handlinger?

Det er klart at Nye Kripos og Telenors satsning på at de største internettleverandørene i Norge om å innføre overgrepsbilderfilter, kan klare å stoppe noe av surfingen på overgrepsbilder. Men som artikkelen i ITpro.no/art/7525.html tar opp, kan blokkering av nettsider gi en falsk trygghet. Personer som virkelig er ute etter overgrepsbildergrafisk materiale, vil sette seg grundig inn i de muligheter som finnes for å unngå disse filtrene. Og det viser seg at mulighetene er mange.

F.eks. Dersom vi skulle prøve å unngå NyeKripos og Telenors filtre, så ville det være naturlig å søke på nettet etter Proxyer (gjerne i utlandet) med høy anonymitet og bruke disse for å få tilgang til nettsider med ulovlig innhold. Forespørselen din sendes da via en slik anonym Proxy som setter inn sin IP-adresse inn i spørringen, henter ressursen og sender denne til klienten. Da er både nettsiden som ble etterspurt og din ISP "lurt".

Det vil bli mer arbeidskrevende for NyeKripos og/eller ISP-en å oppdage at man holder på med noe ulovlig. Usikkerheten for bruker, vil ligge i om loggen fra Proxyene blir frigitt (hvis det føres logg?). og/eller hvis nettstedet man var innom ligger inne med logg over brukerne og den informasjonen som sendes med under ett besøk. Da kan Nye Kripos eller ISP-en få tak i IP-adressene for å spore opp brukerne av de ulovlige sidene.
I en artikkel på www.digi.no , refereres det til en dom mot Tele2 som formidlet såkalte newsgroups(nyhetsgrupper) med innhold av kjønnslig skildringer med barn, dyr e.t.c. som brukerne av disse gruppene hadde sendt. Noe av kritikken som ble framført i dommen, var at de ikke hadde rutiner for å kontrollere om det foregår noe ulovligheter på Nyhetsgruppene og annet materiale som går via ISP-en . I tillegg bør de manuelt godkjenne opprettelse av nye grupper for å unngå at det kaller gruppene for hva de vil.

Vedlegg nr 1 med eksempel fra webside som viser IP – adresser for anonyme Proxyer.

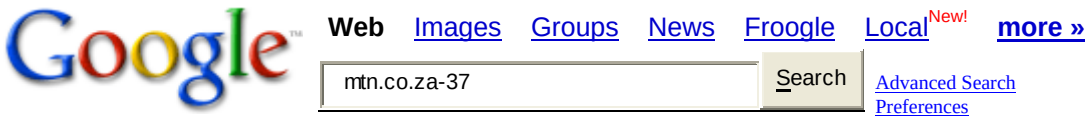
 # 6

1 2 3 4 5 [6] 7 8 9 10 11 12 13 14 15 16 17 18 19 20

211.184.27.161:80	anonymous		Korea(S)
211.114.193.150:8081	anonymous	+	Korea(S)
211.114.193.150:8080	anonymous	+	Korea(S)
211.46.197.60:80	elite proxy	+	Korea(S)
211.43.104.137:444	elite proxy		Korea(S)
211.39.148.41:4480	anonymous	+	Korea(S)
211.34.123.125:8080	elite proxy	+	Korea(S)
210.125.136.32:80	elite proxy		Korea(S)
210.105.204.13:80	anonymous		Korea(S)
203.227.243.162:2578	elite proxy		Korea(S)
134.75.217.55:80	elite proxy		Korea(S)
210.107.249.32:3128	elite proxy		Korea(S)
210.107.249.32:3124	elite proxy		Korea(S)
147.46.240.166:3128	elite proxy		Korea(S)
143.248.139.169:3124	elite proxy		Korea(S)
143.248.139.168:3124	elite proxy		Korea(S)
219.93.211.74:80	anonymous		Malaysia
219.93.190.194:80	anonymous		Malaysia
219.93.72.38:8080	anonymous		Malaysia
219.93.1.210:8080	elite proxy	+	Malaysia
218.208.99.98:6588	elite proxy	+	Malaysia
210.187.110.230:8080	anonymous		Malaysia
210.19.204.245:3128	anonymous		Malaysia
202.1.195.52:8080	anonymous		Maldives
207.248.240.119:80	elite proxy		Mexico
207.248.240.118:80	elite proxy		Mexico
200.78.237.98:80	anonymous		Mexico
200.67.239.225:80	anonymous		Mexico
200.67.149.183:80	anonymous		Mexico
200.56.125.127:80	elite proxy		Mexico
200.39.200.132:80	anonymous		Mexico
200.39.200.132:443	anonymous		Mexico
148.244.150.58:80	elite proxy		Mexico
148.244.150.57:80	elite proxy		Mexico
148.235.6.87:80	anonymous		Mexico
148.233.68.25:80	anonymous		Mexico
148.223.132.121:80	anonymous		Mexico
196.20.24.170:8080	anonymous		Namibia
195.240.163.2:80	anonymous		Netherlands
83.103.43.252:80	elite proxy		Netherlands
82.237.216.153:80	anonymous		Netherlands
82.229.244.15:80	elite proxy		Netherlands
82.229.70.87:6588	elite proxy	+	Netherlands
82.225.61.24:80	anonymous		Netherlands
82.224.250.121:8080	anonymous		Netherlands
82.224.216.83:443	anonymous		Netherlands
82.224.216.83:80	anonymous		Netherlands
62.58.60.74:80	anonymous		Netherlands
217.121.81.109:80	elite proxy		Netherlands
213.53.223.114:444	elite proxy		Netherlands
212.129.143.246:80	anonymous		Netherlands
62.195.74.71:80	elite proxy		Netherlands
165.98.244.34:444	elite proxy		Nicaragua
80.88.131.165:8000	anonymous		Nigeria
193.220.11.147:8080	anonymous	+	Norway
129.242.19.197:3128	elite proxy		Norway
129.242.19.196:3128	elite proxy		Norway
129.240.228.138:3128	elite proxy		Norway

Kilde: http://www.samair.ru/proxy/proxy-06.html

Vedlegg nr. 2 viser eksempel på resultatet av et Googlesøk på domenenavn og IP -adresse:



Sponsored Links

Mtn
Mtn info.
Visit our free investing resource.
www.getbestinfo.com

Web Results **1** - **4** of about **5** for **mtn.co.za-37**. (**0.18** seconds)

- (Fwd) Telkom Call More - Petition URGENT

... Yogi Moodley - moodle_y@**mtn.co.za 37**. Marcus Naidoo - mmnaidoo@fnb.co.za 38. Gertrud Ebner - gebner@fnb.co.za 39. Andriesa du Preez - adupreez@fnb.co.za **...**
www.linux.org.za/Lists-Archives/glug-9909/msg00243.html - 10k - Cached - Similar pages

- Serveur Cache : Frequency of Access to remote sites

... 98174 ww2.ynotnetwork.com : 37 : 117330 www.**mtn.co.za : 37** : 118789 www.lavoixdunord.fr : 37 : 90268 www.tahiti.com : 37 : 531607 www.science-store.com **...**
www.univ-brest.fr/Stats/pwebstat/ cache/weeks/hosts/proxy.28.total-remote-hosts.html - 181k - Cached - Similar pages

- Serveur Cache : Frequency of Access to remote sites

... 16430 www.hq.nasa.gov : 37 : 125654 www.meninuniform.com : 37 : 322039 www.edu.francetelecom.fr : 37 : 121764 www.**mtn.co.za : 37** : 79021 www.bizbank.net **...**
www.univ-brest.fr/Stats/pwebstat/ cache/weeks/hosts/proxy.25.total-remote-hosts.html - 231k - Cached - Similar pages

- User Access Reports

... www.exactmobile.co.za, 16, 250,090, 1.47%, 16.77%, 83.23%, 00:26:43, 1603938, 3.23%, www.**mtn**.**co**.**za**, **37**, 97,751, 0.57%, 10.57%, 89.43%, 00:23:46, 1426881, 2.88%, **...**
unix-01.gcs.co.za/squid/daily/ 18Jul2003-19Jul2003/192.168.2.54.html - 101k - Supplemental Result - Cached - Similar pages

In order to show you the most relevant results, we have omitted some entries very similar to the 4 already displayed. If you like, you can *repeat the search with the omitted results included*.

Internett som verktøy for formidling av overgrepsbilder - bruk av proxy.

IN 116
Samfunnsinformatikk 04/05

Levert av

Gruppe B
Raymond Karstensen
Helge Aurdal
Marius Sagdal
Morten Lein

Vår 2005
HiNe

Forord

Vi i gruppe bravo, som består av 4 medlemmer, går første året på Informatikk Bachelor studiet ved Høgskole i Nesna (HiNe). I faget IN 116 Samfunnsinformatikk 04/05 fikk vi i oppgave å skrive en rapport om oppbygning av proxyer og hvordan dette verktøyet brukes på Internett.

Denne rapporten blir lagt ut for offentlig innsyn, da primært KRIPOS og Redd barna, samt bli lagt ut på Prosjekt Gå inn i din tid sin ressursside.

Dette var ikke et oppdrag fra KRIPOS, men et oppdrag på vegne av HiNe. Derfor peker alle referanser tilbake til HiNe, ikke KRIPOS.

Denne rapporten er laget med veiledning av Per A. Godefjord, faglærer i IN 116 Samfunnsinformatikk 04/05 ved Høgskolen i Nesna.

Helge Aurdal, Raymond Karstensen, Marius Sagdal og Morten Lein
Gruppe bravo

Innledning

Oppgaven vi har fått går ut på å beskrive hva en proxy er, hvordan de fungere og hva de blir brukt til. Noen problemstillinger vi har sett på er :

- ✓ Hva er en proxy?
- ✓ Og Hva er en Anonym Proxy?
- ✓ Hvordan brukes en proxy?
- ✓ Og Hvordan brukes en Anonym Proxy?
- ✓ Hva kan proxyer brukes til?
- ✓ Er man egentlig anonym bak en proxy?
- ✓ Kan proxyer brukes til spredning av overgrepsbildergrafisk material?
- ✓ Brukes proxyer som en del av spredning av overgrepsbildergrafisk materiale?
- ✓ Mulig å få tak i logger som vi kan se på?

Med utgangspunkt i disse problemstillinge håper vi å få svar på hvor stor grad proxyer brukes til spredning av overgrepsbildergrafisk materiale, og kanskje hvordan man kan få stoppet dette

HVA ER PROXY?

En proxy-server er et mellomledd mellom din maskin og Internett. Dvs at når du besøker en internettside går forespørselen gjennom en proxy-server (forutsatt at systemet er konfigurert for å gjøre det).
La oss si at du skal besøke www.vg.no. Nettleseren din tar først kontakt med proxy-serveren før den henter ned et dokument eller en fil. Hvis ikke proxyen har det ønskede dokumentet laster den ned dokumentet og lagrer det i minnet. Samtidig overføres dokumentet til din nettleser. Neste gang du besøker vg.no sjekker proxyen om dokumentet finnes i minnet. Hvis dokumentet finnes i minnet kontaktes serveren hvor dokumentet kommer fra og sjekker om det er blitt endret. Dersom dokumentet ikke er forandret sendes dokumentet fra proxyen til nettleseren i stede for å hente fra vg.no sin server.
En proxy-server blir ofte administrert av en administrator. Administrator kan sette opp proxyen til å filterere trafikken som går gjennom proxy-serveren. Dvs at admin kan stenge ute de internettsidene han/hun vil.
Proxy-server brukes av 3 grunner.

1. Økt responstid for klienter
2. Sikkerhet/anonymitet
3. Oppheve begrensinger satt av ISP

Økt responstid for klienter

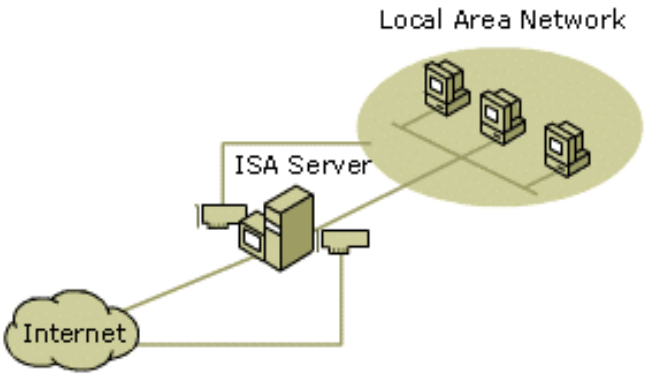
Siden proxyen lagrer websiden som besøkes i en såkalt ”cache”, det vil si i kortminnet til proxyen, vil dette øke hastigheten og man slipper å laste ned siden fra Internett (med mindre den er endret. Se over.). På denne måten sparer man båndbredde.

Sikkerhet/anonymitet

Det finnes 2 hovedtyper proxy. Proxy og anonym proxy. Ved bruk av en anonym proxy vil ikke maskinens IP-adresse være synlig for andre bruker på Internett. De vil kun se IP-adressen til den anonyme proxy-serveren. Ved bruk av proxy vil ikke bare IP-adressen til proxyen være synlig, men også IP-adressen til maskinen bak proxyen(Se lengre ned i rapporten for bedre forklaring).
En proxy/anonym proxy kan benyttes i 2 situasjoner: internt i et lokalt nettverk eller som webproxy på Internett. Er en proxy/anonym proxy satt opp internt i et nettverk vil ikke klientene i nettverket være synlig for omverdenen. Dette betyr at man surfer anonymt på Internett, og en hacker vil ikke kunne identifisere IP-adressen, nettleser, operativsystem eller annen informasjon til en bedrifts pc-er.
Måten dette gjøres på er at proxyen bytter ut ip-adressen til klienten med sin egen IP før forespørselen sendes ut på Internett. Når proxy-serveren får svar tilbake byttes IP-adressen tilbake for så å sendes til klienten.

Oppheve begrensinger satt av ISP

Er en proxy-server satt opp som en webproxy vil denne kunne brukes av nettlesere og andre programmer som bruker Internett som kommunikasjonskanal. Scenarioet er det samme som over. Du sender en forespørsel ut på Internett der målet er proxy-serveren. Proxy-serveren setter sin IP-adresse inn i spørringen, henter ressursen, og sender denne tilbake til klienten. På den måten "lures" både nettsiden du spurte etter, og din ISP.



Forskjellige typer proxy

HTTP Proxy
Dette er den mest brukte proxytypen.

Tidligere med hjelp av denne typen proxy var det bare mulig å se websider, bilder og laste ned filer. Nå har nye programversjoner som feks ICQ og MSN funnet ut hvordan de kan jobbe seg gjennom HTTP Proxyen. Alle browsere vet nå hvordan de jobber forbi denne typen proxyer. Når man sender en request til en webside er det en del informasjon om deg som sendes samtidig. Dette kan være hvilket OS du bruker, hvilken browser og dens konfigurasjon, IP-adressen og annen informasjon.

HTTP proxy servere har flere forskjellige nivåer med anonymitet. Det er ikke alltid først og fremst anonymiteten som er viktigs, dette kommer helt an på hva proxyen brukes til. Du kan dele inn de fire forskjellige nivåene slik:

- ”Transparent”(Proxy): Disse proxyene er ikke anonyme. Den lar først webserveren vite at det brukes en proxy server, så ”gir” de IP-adressen til en klient. Oppgaven til en slik proxy er stort sett å cache informasjon og/eller å skaffe internett tilgang for flere maskiner via en enkel tilkobling.

- ”Anonymous” (Anonym proxy): Denne typen servere lar en servermaskin(webserver) vite at det brukes en proxy, men gir ikke ut noen IP-adresse fra klienter.

- ”Distorting” (Fordreide proxy): Ulikt fra den forrige typen, overfører denne en IP-adresse til serveren. Adressen den sender er derimot ikke din, den er generert av proxyserveren og er en veldig lang adresse som er helt tilfeldig. Dermed gjør denne typen din IP-adresse ugjenkjennelig fra webserverens posisjon.

- ”High anonymity”(Avansert anonym proxy): Den fjerde og siste varianten sender heller ikke IP-adressen din til webserveren. Forskjellen fra de andre er at den informerer ikke serveren om at den bruker en proxyserver. Dermed tror web-serveren at den jobber direkte med en klient.

HTTP proxyer kan organiseres inn i såkalte ”chains” på godt norsk kalt lenker. Dette vil gjøre anonymiteten mye høyere på Internett. Men det er ikke bare positive sider ved lenkene. En slik konstruksjon kan lage en hel del problemer. Hovedproblemet med dette er at for tilkoblingen inn til en lenke må man bruke spesielle programvarer.

Browsere og stort sett alle andre program vil ikke tillate å lage og bruke lenker av proxyservere. For å organisere proxyer inn i en lenke må man lage en ”tunnel” som går gjennom en HTTP proxy. Når du bruker denne tunnelen, lager programmet ”en sti” gjennom noen proxy servere til en spesifikk webserver. Bortsett fra å sende forespørsler gjennom tunneler, bør en HTTP proxy støtte Secure Sockets Layer(SSL). Dette er en ”ferdighet” som er laget for å beskytte tilkoblinger fra å bli stoppet eller dekodet. Bortsett fra beskyttelse, tillater SSL deg å organisere en ”tunnel” gjennom en lenke av proxy servere. SSL brukes ofte av banker og betalingssider.

Når du oppretter en slik lenke av proxy servere, kan du koble til mange andre typer proxyer. Som for eksempel SOCKS og CGI som forklares lengre ned. Det er viktig å plassere HTTP proxyen i rett posisjon i lenken. Det bør stå en SOCKS proxy først i lenken.(om den er tilgjengelig), HTTP proxyen må bør i så fall altså stå som nr to og så setter CGI til slutt.(viss den er tilgjengelig). Dette fordi man setter de opp etter hvilke oppgaver de gjør best og hva de støtter. Lenkene kan da bli seende ut som eksemplene under:

- SOCKS proxy > > > > HTTP proxy > > > > CGI proxy
- SOCKS proxy > > > > HTTP proxy
- HTTP proxy > > > > CGI proxy

Anonymitet til HTTP proxyer

Type Info	Proxy Type	Ingen	Transparent	Enkel	Fordreide	Avansert
|	-----→	Proxy	Proxy	Anonym	Proxy	Anonym
V				Proxy		Proxy
REMOTE_ADDR		Din IP	Proxy IP	Proxy IP	Proxy IP	Proxy IP
HTTP_VIA		Ikke bestemt	Proxy IP	Proxy IP	Proxy IP	Ikke bestemt
HTTP_X_FORWARDED_FOR		Ikke bestemt	Din IP	Proxy IP	Random IP	Ikke Bestemt

REMOTE ADDR: Ip adressen til en klient.
HTTP_VIA: Adressen til proxy-serveren. Blir satt at proxyen. Er den Ikke bestemt brukes ikke proxy.
HTTP_X_FORWARDED_FOR: Den egentlige IP til en klient(din IP). Blir også satt av proxyen. Er den Ikke bestemt brukes ikke proxy.

SOCKS Proxy
Disse proxy-serverne vet hvordan den skal arbeide med stort sett all informasjon på Internett (TCP/IP protocoll), men for bruk i programmer bør det være indikert en evne for å jobbe med socks proxy. Noen tilleggsprogrammer er nødvendige for å bruke socks proxier i browsere. (De forskjellige browserne vet ikke hvordan de skal jobbe seg gjennom en socks proxy.) Likevel fungerer alle versjoner av snakke program som MSN og ICQ ++ uten problemer med socks proxyer. Anonymiteten er veldig høy.

Når det kommer til anonymiteten, så er det slik at når proxyen overfører all dataen til fra en klient til en server, så vil webserveren tro at SOCKS proxyen selv er en klient. Derfor blir anonymiteten til en slik type proxy veldig høy.

En SOCKS proxy overfører data mellom maskiner uten å forandre på innholdet. Dette gjør at de veldig enkelt tillater å lage lenker med flere SOCKS proxy servere på vilkårlige lengder. Det er derimot nødvendig med spesielle programmer for å lage slike lenker, ettersom vanlig programvare bare takler bruken av *en* SOCKS proxy om gangen.

Det er mulig å koble SOCKS proxyer i lenker (chains). Du kan koble de sammen med de andre typer proxy servere som CGI og HTTP i disse lenkene, men da må SOCKS proxyen stå først i lenken for at det skal fungere.
Du kan altså koble de slik som under:

- SOCKS proxy > > > > HTTP proxy > > > > CGI proxy
- SOCKS proxy > > > > HTTP proxy
- SOCKS proxy > > > > CGI proxy

Men ikke slik:

- HTTP proxy > > > > SOCKS proxy > > > >CGI proxy
- CGI proxy > > > >SOCKS proxy.

CGI Proxy (anonymiserer)
Denne typen proxy server kan man koble til kun med en browser. Web-basert proxy-server. Dvs man må inn på en nettside som tilbyr en slik proxy server. En slik side vil antakeligvis se ut som en søkeside med en ”Go” knapp. Man skriver inn den ønskede adressen og trykker på knappen. Så vil man bli sendt til denne siden og man vil være helt anonym. I andre programmer er det veldig komplisert å koble seg til. Det er heller ikke nødvendig ettersom man heller kan bruke HTTP proxyer. Ettersom denne typen proxy er ment og designet for operasjoner gjennom browsere, kan man bruke den på en veldig enkel måte. Anonymiteten er den samme som for HTTP proxyer (se over). CGI proxy støtter HTTP og som oftest FTP protokoller.

Når det kommer til anonymiteten er CGI proxyer, gjelder akkurat det samme som for HTTP proxyer. For å oppsummere det kort(En mer detaljert versjon står under HTTP), det er 4 forskjellige typer.
Disse 4 proxy typene kan deles inn i 3 forskjellige *kategorier*:

- *Transparent Proxies*: Proxy som ikke gjemmer informasjon om din IP.

- *Anonymous Proxies*: Enkel anonym proxy som ikke legger skjul på at en proxy blir brukt, men som skjuler din IP.

- *Fordreide proxy*: legger heller ikke skjul på at en proxy blir brukt, men erstatter din IP med en helt tilfeldig(random) IP. Alle proxyer som skjuler din IP kalles anonyme proxyer.

- *High Anonymous Proxies*: Avansert anonym proxy som skjuler at du bruker proxy. Har samme verdier som om man ikke bruker proxy, bortsett fra at din IP blir erstattet med proxy IP.

Du slipper å forandre på innstillinger i browseren når du skal installere tilleggsprogrammer eller lignende med CGI proxy. Det er nok å åpne et internettside med CGI proxy i et browservindu. Der skriver du inn den URL som trengs og trykk ”Go”. Ulempene med CGI proxyer er at den har begrenset støtte til FTP og noen ganger vil ikke en CGI proxy tillate å vise bilder.

Du kan også lage proxy lenker med CGI proxy. Det er veldig enkelt som med alle de andre proxyene. Du kan ha et hvilket som helst ønsket antall med CGI proxyer organisert inn i lenken. CGI proxyer kan kobles opp mot de fleste andre typer proxyer, men det er viktig at CGI proxyen er den siste proxyen i lenken. Under finner du eksempler på hvordan du kan du organisere lenkene:
- SOCKS proxy > > > > HTTP proxy > > > > CGI proxy
- HTTP proxy > > > > CGI proxy
- SOCKS proxy > > > > CGI proxy

Ettersom CGI proxyen må stå sist kan du ikke organisere de slik:
- CGI proxy > > > > SOCKS proxy
- SOCKS proxy > > > > CGI proxy > > > > HTTP proxy
- CGI proxy > > > > HTTP proxy

Surfing ved bruk av CGI-proxy

Vi besøkte websiden http:\\www.the-cloak.com som tilbyr gratis surfing med CGI-proxy, og prøvde å surfe anonymt. Sjekket ip-adressen vår ved å skrive inn http:\\www.ipadresse.no i URL-feltet vi fikk beskjed om å fylle ut. Bildet viser det svaret vi fikk og ip-adressen som de fant er ikke vår IP-adresse. Dette skulle da bety at CGI-proxy fungerer. Foretok en DNS søk på IP-adressen og fikk den sporet tilbake til The Cloak sin server. Etter det vi kunne se så var vi sendt igjennom 3 andre servere.

Reverse DNS for 216.127.72.7

Generated by www.DNSstuff.com

```
Location: UNITED STATES [City: San Francisco, California]
Anonymous IP: the Cloak

Preparation:
The  reverse DNS entry for an IP is found by reversing the IP, adding it to "in-addr.arpa", and looking up the PTR record.
So, the reverse DNS entry for 216.127.72.7 is found by looking up the PTR record for
 7.72.127.216.in-addr.arpa.
All DNS requests start by asking the root servers, and they let us know what to do next.
See How Reverse DNS Lookups Work for more information.

How I am searching:
Asking f.root-servers.net for 7.72.127.216.in-addr.arpa PTR record:
       f.root-servers.net says to go to chia.arin.net. (zone: 216.in-addr.arpa.)
Asking chia.arin.net. for 7.72.127.216.in-addr.arpa PTR record:
       chia.arin.net [192.5.6.32] says to go to ns1.ev1.net. (zone: 72.127.216.in-addr.arpa.)
Asking ns1.ev1.net. for 7.72.127.216.in-addr.arpa PTR record:  Reports www.the-cloak.com. [from 216.88.76.6]

Answer:
216.127.72.7 PTR record: www.the-cloak.com. [TTL 28000s] [A=216.127.72.7]

To see the reverse DNS traversal, to make sure that all DNS servers are reporting the correct results, you can Click Here.
```

Spredning av bilder og annet materiell

Proxy-filter

Siden man kan sett opp filter på en proxy-server betyr det at man kan stenge ute hvilken som helst internettside. Man kan f.eks konfigurere serveren til å kun slippe igjennom VG Nett sine sider i en peroiden på 2 timer om dagen. F.eks fra 08-10 på morgenen. Dette betyr også at man kan stenge ute allesider med overgrepsbilder. Noe som i stor grad er med på å forhindre distibusjon av bilder og annet materiale.
Ved at mange av de store ISP'ene nå innstalerer filter for å filterere bort nettsteder som distribuerer overgrepsbildergrafisk materiale tror Fredrik Syversen dette kommer til å ramme den komersielle siden av denne type kriminalitet. Han mener også at det er viktig at et slikt samarbeid ikke bare fungere nasjonalt, men også at man får til et samarbeid for lignende konstellasjoner i Europa. [41]

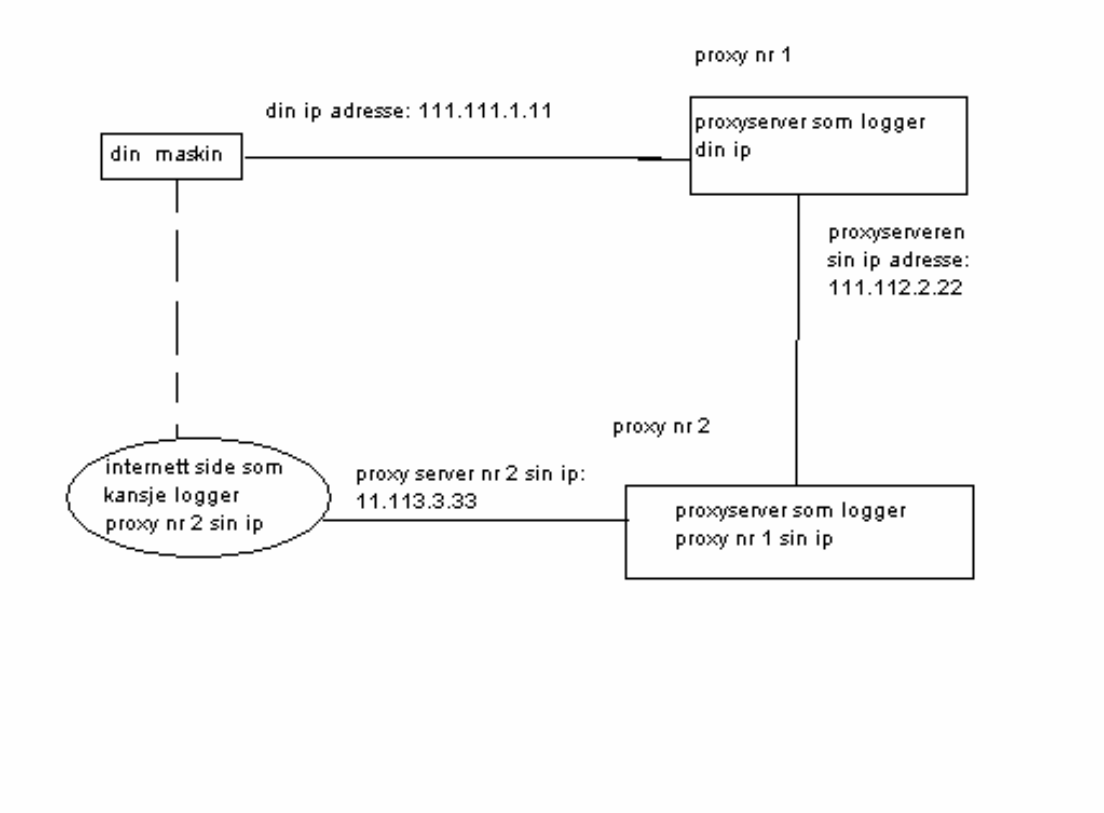
Proxy - En stopper eller en hjelper?

En proxy i dag kan være en både en stopper og en hjelper når det gjelder spredning av bilder.

Hvis man sitter bak en proxy så vil all trafikk ut mot Internett bli kjørt gjennom proxyen og loggført. Dette betyr også at man kan filtrere trafikken ut mot Internett. En måte å gjør dette på er å installere et filter. Se avsnitt "Samarbeid mellom Nye KRIPOS og 5 store ISP". Det betyr at du kan stenge ute sider som man vet inneholder overgrepsbildergrafisk materiale. Andre måter å stoppe distribusjon av slikt materiale er å stenge bruken av IRC, MSN, ICQ og andre chatte program. Man kan stenge ute news-grupper som mange bruker til å distribuere slikt materiale. Det er mange måter å gjøre det på.
Selv om det finnes mange måter å begrense distribusjon av overgrepsbildergrafisk materiale på, vil det kun stoppe fåtallet. For det finnes måter å komme seg forbi proxy-servere.
Siden overgrepsbilder er ulovlig å distribuere så vil man ønske å skjule seg så godt man kan for resten av internettverden. En måte å gjør dette er ved å bruke flere proxier. Høres kanskje litt rart ut, men det er sant. Ved å bruke flere proxyer eller proxy-chaining som det heter, vil det kunne se ut om du ligger bak en annen proxy enn det du egentlig gjør. Finnes også Java-programmer blant annet som kan kjøre utenom proxyen, uten at vi ska gå nærmere inn på dette.
Men selv om det tilsynelatende ser ut som man blir anonym, så vil man aldri bli helt anonym. En proxy vil logge all trafikk ut mot Internett og dette betyr at man se hva en bruker har surfet på. Så selv om en proxy-server kan gjøre deg nærmest anonym, så er det mulig å få tak i deg. Du kan gjemme deg bak mange proxy-servere, men organer som f.eks Krips vil finne deg til slutt. Det tar bare litt lengre tid og flere ressurser.

[41] Fredrik Syversen, "Internettbransjen til felles kamp mot overgrepsbilder", IKT Norge
http://www.ikt-norge.no/templates/Page.aspx?id=524

Nedenfor vil du se et bilda av hvordan proxy-chaining fungere. Her har da en bruker prøvd å gjemme seg bak 2 proxyer, og som du ser så er det enkelt å spore tilbake til brukers maskin.



Den strippete linjen viser den veien du ville tatt uten å koble deg til proxyer og da vil den siden ha din IP adresse isteden for proxy server nr 2 sin. Slik kan du gjemme deg bak en del proxyer og finne overgrepsbilder på sider og spre den.

En proxy server kan også gjøre deg tilnærmet anonym på Internett (når jeg skriver nærmest lik mener jeg at KRIPOS og slike organer vil finne deg, det tar bare litt lenger tid og penger.) Hvis du gjemmer deg bak en hel rekke av disse åpne proxyene så tar det lengere tid for folk kan finne deg. Det jeg prøver å si er at jo flere proxyer du gjemmer deg bak jo lenger tid tar det for folk (organer) og finne deg, men som jeg nevnte ovenfor så logger proxyer og de vil logge ip adressen din som du ser på fig 1. og det er slik de finner deg. De ser at proxy nr 2 har vært på siden får tak i loggen til proxy nr 2 og finner ut at proxy nr 1 har vært tilkoblet og så får di tak i proxy nor 1 sin logg og dermed finner de deg.

Samarbeid mellom NyeKRIPOS og 5 store ISP

Fem store internettleverandører, Freewave, NextGenTel, Tele2, Telenor, og UPC har startet et samarbeid med Nye KRIPOS. Løsningen bygger på Telenors filter som har vært i drift siden november 2004. Disse 5 selskapene har installert et filter på sine servere som blokkerer trafikk mot kjente overgrepsbildersider. Selskapene står for den tekniske driften, mens det er Nye KRIPOS som overfører lister over nettsteder som relateres til distribusjon av overgrepsbildergrafi til de enkelte selskapene. Så dersom en kunde prøver å åpne en side som inneholder overgrepsbildergrafisk innhold kommer det opp en sperreside med informasjon om

filteret, samt en lenke til KRIPOS. Til nå er flere hundre sider med ulovlig barnpornografisk innhold registrert av KRIPOS.
Selv om dette høres ut som et bra tiltak, som det da er, vil ikke filteret stoppe alle. Filteret vil ikke stoppe spredning via e-post og fildelingsprogrammer. Filteret vil heller ikke registrere hvem som forsøker å åpne internettsiden.

Selv om selskapene står for driften av filtrene har de noen regler som må følges.
Hentet fra denne adressen: http://www.digi.no/php/art.php?id=210096
Slik er reglene:

- Tilbyderne skal ikke utøve noen form for generell overvåking eller domstolslignende oppgaver i form av å vurdere lovligheten av innhold som formidles av andre, utover det som følger av gjeldende retts aktsomhetskrav.

- Tilbyderne utviser en proaktiv holdning overfor det innhold som formidles, for eksempel ved spredning av innhold av typen overgrepsbildergrafi.

- Tilbyderne logger ikke IP-adressene som benyttes, og kan således ikke tilbakeføre dette til abonnentene

- Distribusjon via fildeling, e-post og liknende vil ikke bli påvirket av filteret.

Kriminalitet på Internett blir stadig mer utbredt, og har sannsynligvis eksistert fra dagene da Internett ble født i et mindre eller større omfang. De kriminelle utnytter i stor grad den teknologiske utviklingen innen kommunikasjon og datateknologi og de ligger ofte flere hakk foran politiet - noe som vanskeliggjør politiets arbeid.
De færreste bruker sitt virkelige navn som avsender når kriminelle handlinger blir begått,(enten det er snakk om amatører eller profesjonelle kriminelle) og de prøver å tilsløre og forfalske all informasjon som kan føre handlingen tilbake til dem.
Hvis det viser seg at den kriminelle bruker en Norske ISP (Internet Service Provider) vil det bli tatt kontakt med denne for å se på trafikkdata hvilken person som var logget på til hvilket tidspunkt. Det er svært viktig at dato og tid for ulovlighetene er nevnt et eller annet sted i tipset for å kunne spore dette.
Trafikkdata er logger som tele/nettoperatørene har på klientene sine som bl.a. inneholder hvem som har logget på Internett til hvilken tid, hvor de har vært og hva de har lastet ned. Å få innsyn i trafikkdata er et stort problem.

Metodeutvalget foreslår at innsyn i slike trafikkdata først skal gis ved lovbrudd hvor straffen er 3 år eller mer, mens spredning og besittelse av overgrepsbildergrafi bare straffes med 2 år. Dette kompliserer eller gjør arbeidet umulig å fullføre. Metodeutvalget foreslår at strafferammen økes til minst 3 år for slik virksomhet.

Proxy logger

Vi sendte over 50 mailer til forskjellige oppgitte adresser til proxyer rundt omkring i verden. Vi brukte lang tid på å vente på svar, men det var ikke mye positive svar å få. Det endte med at vi måtte gi opp å vente på logger, og begynte med andre oppgaver. Følgende mail ble sendt ut til de forskjellige proxyeierne:

Hello,

We're a group of students at Nesna University College, based in Nordland in the middle of Norway. Our assignment is to attain knowledge about how proxy servers work and how they are used in the real world. This is a group assignment in a class called "Social Informatics" and concerns how IT is used within the social parameters. This is why we are writing this email to you, we're acquired to obtain proxy logs from several proxy around the world, go through these and see if there is any foul use of the internet through these proxy's. We will also see to that the obtained information would only be used in this assignment and not for other purposes.

We would be very obliged if you were able to help us obtain this information and help us solve this assignment, as it is very crucial for our final grade in this class.
We'll be looking forward to your reply.

You might be able to verify our sincerity by opening the following link:
http://it-mo.hinesna.no/~pag/pag/engelsk.html

Our Associate professor is called Per A. Godejord and he will be grading us on our assignment.

Yours sincerely,

Morten Lein on behalf of group Bravo
Nesna University College,
Nordland,
Norway

- Det eneste fornuftige svaret vi fikk, bortsett fra alle de mailene som ikke nådde frem og de med automatisert svar mailene, var dette svaret som ligger under her:

*Thank you for your request for the log/history file from IP: ***.**.***.**.*

*Lookup services document the State of Georgia/Board of Regents as the Point of Contact for the IP address (***.**.***.**).*

*The IP address you reported (***.**.***.**) is currently in use by a Georgia Public Library System (GPLS) site. Customer Services will forward your request to the site administrator and will respond to you.*
This request is recorded in Customer Services case 219335.

Vi hørte dessverre aldri mer fra denne proxyeieren.

Det er sikkert flere forskjellige grunner til at vi ikke hørte mer fra Proxy-eierne vi hadde sendt mail til. Hovedgrunnen hos de fleste er nok at de vil beskytte kundene sine og deres "privatliv". Det er mange som driver med alt fra små ulovligheter som privatkopier eller lignende, til store ulovligheter som for eksempel overgrepsbilder. Disse kundene vil jo ikke fristes veldig av deres Proxy når de vet at de gir ut logger og lignende til hvem som helst. Dette er jo selvfølgelig ikke fordi de vil tillate uloveligheter, men fordi de vil gi alle kundene sine den tryggheten om at ingen overvåker dem. Det kan ogsÂ være at den mail-adressen de har gitt ut på nettet, ikke sjekkes av en person, men av en datamaskin. For det var kanskje 80% av mailene vi ikke fikk svar på. Eller at vi bare fikk et autosvar som det sto et eller annet ferdigskrevet på. Dette blir også et videre problem for KRIPOS, som hadde hatt en mye enklere jobb om de fikk vite om at det ble sendt forespørsler, om Â få åpnet internettsider med ulovlig materiale.

Dessverre har vi ikke fått tak i noen logger. Dette fordi ingen vil gi ut slik informasjon. Bakgrunnen for at Internett leverandørene vi har kontaktet ikke vil oppgi denne informasjonen er at de vil verne om sine kunder og sørge for et godt forhold til sine kunder. Av alle kundene så kan vi anslå at det er bare noen få som faktisk holder på med ulovlige ting, for eksempel overgrepsbilder. Det vil også være mot norsk lov om personvern og i strid med dataloven å gi ut informasjon til hvem som helst. Etter en samtale med en ansatt i en lokal Internett leverandør bedrift uttalte han at det skulle mye til for at de gav ut disse loggene, og at man kun gjorde dette hvis det forelå en dom fra en domstol om at disse loggene skulle utleveres. Hvis politiet kom bankende på døra og krevde disse loggene vil de sannsynligvis ikke fått utlevert disse.

Vi mener at personopplysningsloven gir støtte til ISP-ene i å ikke gi fra seg loggene uten videre. Men nå er det jo ting på gang fra EU som gjøre at logger må lagres lengre og at politiet vil kunne kreve å få loggene utlevert.

Før vi går videre skal vi sitere to aktuelle paragrafer fra personopplysningsloven.

§ 8. *Vilkår for å behandle personopplysninger*

Personopplysninger (jf. § 2 nr. 1) kan bare behandles dersom den registrerte har samtykket, eller det er fastsatt i lov at det er adgang til slik behandling, eller behandlingen er nødvendig for

a) å oppfylle en avtale med den registerte, eller for å utføre gjøremål etter den registrertes ønske før en slik avtale inngås,
b) at den behandlingsansvarlige skal kunne oppfylle en rettslig forpliktelse,
c) å vareta den registrertes vitale interesser,
d) å utføre en oppgave av allmenn interesse,
e) å utøve offentlig myndighet, eller
f) at den behandlingsansvarlige eller tredjepersoner som opplysningene utleveres til kan vareta en berettiget interesse, og hensynet til den registrertes personvern ikke overstiger denne interessen.

I tillegg er følgende paragraf aktuell:

§ 15. *Databehandlerens rådighet over personopplysninger*

En databehandler kan ikke behandle personopplysninger på annen måte enn det som er skriftlig avtalt med den behandlingsansvarlige. Opplysningene kan heller ikke uten slik avtale overlates til noen andre for lagring eller bearbeidelse.

I avtalen med den behandlingsansvarlige skal det også gå frem at databehandleren plikter å gjennomføre slike sikringstiltak som følger av § 13.

Vi mener jo som sagt tidligere at ISP-ene kan nekte å levere fra seg loggene med støtte i personopplysningsloven, og da særlig ut fra de to paragrafene over.

Men hva mener bransjen selv? Vi spurte en representant.

Hvorfor ingen vil gi ut logger – et intervju med en ISP-ansatt

Vi kontaktet en ansatt ved en bedrift som leverer bredbånd til et stort omfang med kunder for å bekrefte dette. Den ansatte ønsker å være anonym av egne grunner, derfor blir personen referert til som ”den ansatte”.

Den ansatte kunne bekrefte våre påstander om at de ønsker å verne om sine kunder ved å ikke gi ut slike logger til hvem som helst som ønsker å få tak i dem. Den ansatte utdypet videre med å forklare grunnen til dette.

”Hva kunden bruker sin Internett tilgang er helt og holdent opp til kunden selv, om det så gjelder vanlig kontorbruk, altså lesing av nettaviser, research etc., eller om det gjelder andre lovlige sider med et bestemt innhold. Det er ikke bedriftens ansvar å leke politi ovenfor sine kunder, da de ikke har lov til dette i henhold til personopplysningslovens paragraf § 8 og § 15.”

Videre fortsetter den ansatte med å utdype hvilke fordeler og ulemper dette har i forhold til ulovligheter, som overgrepsbilder etc.

”Det hele er en vinn-tap situasjon, da man greier å beskytte privatlivet til mesteparten av kundene, så greier man å gjemme ulovlighetene til et fåtall.

Hvis man tok et utsnitt på 1000 kunder fra kunderegisteret, så ville kanskje 1-2 % av disse drive med ulovligheter som overgrepsbilder. Men for å komme fram til disse må en gå igjennom alle de som ikke gjør noe som bryter med norsk lov, og greier å holde seg innenfor lovverket, selv om det kan forekomme ting som anses som tabu og lignende for andre, ting man helst vil holde hemmelig for andre. Vi anser også at temaer som overgrepsbilder, incest og lignende er et mye større problem og ikke minst et mye mer alvorlig problem på internett enn at kunder driver å laster ned piratkopiert materiale via nettet. Det er viktigere for oss som bedrift å få stanset disse syke forbryterne enn å drive en heksejakt for diverse plate- og spillselskaper mot ungdommer, slik at de selv kan kapitalisere ytterligere.

Lovverket som det er nå er veldig bra i mine øyne, bedrifter som leverer bredbånd til et stort antall kunder slipper å leke politi ovenfor sine egne og dermed miste klientell på grunn av mistillit mellom leverandør og bruker. Men hvis i fremtiden at en slik lov skulle bli vedtatt, at alt man gjorde av ulovligheter ble loggført og overlevert til politiet med jevne mellomrom, ville det vært som gjenoppstandelsen av Det Tredje riket, i elektronisk form.”

Dette er altså slik en ansatt i en av Norges ISP-bedrifter ser det, og vi velger å avslutte rapporten med det. Så får leserne selv gjøre seg opp en mening om ISP-enes holdning til det å levere fra seg logger, og om vi virkelig er anonyme på Internett når vi bruker anonym proxy.

Referanse- og litteraturliste

Nettsider:

- http://www.computerworld.no/index.cfm/fuseaction/artikkel/id/29789
- http://www.multinet.no/abon_proxy.shtml
- http://itpro.no/art/7525_printable.html
- http://www.digi.no/php/art.php?id=210096
- http://www.stayinvisible.com/index.pl/anonymity_of_proxy
- http://www.the-cloak.com
- http://pekosoft.nux.at/webalizer/pekosoft.nux.at/search_200501.html
- http://pekosoft.nux.at/webalizer/

Epilog

Per A. Godejord
Førstelektor

Prosjekt ”Gå inn i din tid!” er inspirert av et dikt Nordahl Grieg skrev ved starten av den spanske borgerkrig (1936 – 1939).
På forsiden av dette heftet har vi brukt et bilde av en av de mange politiske plakatene fra den spanske borgerkrig, men med en liten endring i teksten.

I stede for å slå fast at å forsvare Madrid er det samme som å forsvare Katalonia, spør vi om det å forsvare anonymitet er det samme som å forsvare overgrep mot barn.

Mens den spanske borgerkrig vekket ungdommer fra hele verden til dyst mot fascismen, vekker kampen mot seksuelle overgrep mot barn knapt nok overskrifter i media.

Riktignok kan aviser ta frem krigstypene dersom politi i flere land slår til med massearrestasjoner etter en vellykket aksjon både på og utenfor Internett, men den daglige kampen mot slike overgrep forbigås i taushet.

I motsetning til da den spanske borgerkrig raste, samles ikke ungdom fra alle verdens hjørner til kamp og våre politikere virker lite villig til å bidra med annet enn ord.

Kampen mot seksuelle overgrep mot barn og bruken av Internett som videreformidlings- og møtekanal av overgrepsbilder er en viktig kamp. Og som alle slike kamper blir den fort preget av svart-hvitt holdninger, der ethvert synspunkt som ikke umiddelbart kan defineres som for, blir kategorisert som mot.

Som forelesere og studenter i samfunnsinformatikk er det vår plikt å både kjempe mot seksuelle overgrep mot barn, og for retten til anonymitet på Internett. Alle har vi en soleklar rett til privatlivets fred når vi surfer i cyber space.

Denne retten er imidlertid ingen rett til å begå kriminelle handlinger eller å videreformidle lidelse og fornedrelse av andre. Det å ha frihet til å være anonym er en frihet med ansvar. Et ansvar for å bekjempe tyranniet enten det er i form av totalitær overvåking av borgere eller seksuelle overgrep mot barn.

Om forfatterne

- Roy Thoresen
- Ole-Jonny Johansen
- Steinar Kulstad
- Arnt Håvard Pettersen
- Felicia Dziales
- Svein Erik Molberg
- Jarle Hagavei
- Hans Petter Hammer
- Jørn Ivar Remmen
- Raymond Karstensen
- Helge Aurdal
- Marius Sagdal
- Morten Lei
- Kjell-Magne Kristiansen
- Einar Selnes
- Kenneth Nerdal
- Eva Daabach
- Unni Pedersen
- Ronny Pedersen

Alle rapportforfatterne er studenter ved første året IT-bachelor, ved Høgskolen i Nesna sin avdeling på Mo i Rana.

Studentene er de første ved HiNes IT-studie som har utført oppgaver etter en ide av NyeKRIPOS, og de er de eneste studentene ved noe høgere utdanningsinstitusjon i Norden som aktivt har jobbet med problematikken rundt seksuelle overgrep mot barn og bruken av IKT som verktøy for distribusjon, lagring av overgrepsbilder og kontakt mellom offer og overgriper. Prosjektet ”Gå inn i din tid!” er helt unikt i nordisk sammenheng, og bygger på et faglig samarbeid mellom Redd Barna og seksjon for informatikk ved Høgskolen i Nesna, der også NyeKRIPOS er en verdifull støttespiller.

Men de viktigste deltakerne er våre studenter. Uten dem hadde vi ikke hatt noe prosjekt. Studentenes innsats, fra de første som deltok i starten av prosjektet (Samfunnsinformatikk ved tredjeår IT-bachelor) i 2003 til årets førsteårsstudenter, har vært formidabel.

Studentene har grunn til å være stolte av seg selv, og vi ved seksjon for informatikk er i alle fall stolte av dem!

Om redaktøren

Per Arne Godejord (f. 1965),
førstelektor i informatikk ved Høgskolen i Nesna.

Faglærer i samfunnsinformatikk ved førsteår IKT-bachelor og IKT for lærere 1, og ansvarlig for prosjekt ”Gå inn i din tid!”.

Utdannet med hovedfag i informasjonsvitenskap, mellomfag i offentlig rett, samt i juridisk spesialfag politirett og pedagogisk seminar ved universitetet i Bergen.

Forfatter av en rekke publikasjoner om IKT og sikkerhet ut fra brukerperspektiv, jus og læring.