Nettpiratene

Dagbladet

Metoderapport - Dataskup 2018

Audun Hageskal - Journalist audun.hageskal@dagbladet.no tlf 48151238
Tor Henning Ueland - Utvikler tor.henning.ueland@aller.com tlf 98005152

Innholdsfortegnelse

Innledning

Piratkopiering har eksistert i flere tiår, og like lenge har kampen mot ulovlig kopiering og spredning av materiale med opphavsrett pågått. De siste 15-20 årene har særlig ulovlig digital spredning av film, tv-serier, spill og musikk via internett vært et mye omtalt problem som rettighetshaverne ikke har klart å bekjempe. Bransjen ser årlig på flere hundre millioner kroner i tapte inntekter som følge av nettpiratene.

I et forsøk på å ta opp kampen mot ulovlige fildelere, trådte en ny versjon av åndsverkloven i kraft i Norge i 2013. Denne slo fast at kopiering og spredning av nettopp fildeling av opphavsrettsbeskyttet materiale er ulovlig. Loven ble raskt kjent som Piratloven. Året før hadde også den *lovlige* strømmetjenesten Netflix blitt lansert her til lands.

Vårt overordnede mål med dette prosjektet, har vært å undersøke status for ulovlig fildeling i Norge, fem år etter at loven som skulle redde film-, tv- og musikkbransjen trådte i kraft. Sentrale spørsmål har vært **hvor utbredt** er piratkopiering og deling i dag, **hvem** gjør det, **hvorfor** gjør de det, **hvor** bor de (er det et by-/bygdefenomen?), **hva** deles, **hvor mange** og **hvem** blir faktisk straffet, **hvem** forsøker å stoppe dem og **hvordan** - og **hva** gjør politiet.

De siste årene har flere og flere lovlige tjenester kommet på markedet, noe som påstås å ha redusert piratkopieringen betraktelig, spesielt innenfor musikk og spill-bransjen. I februar 2018 pågikk en kamp i rettsvesenet rundt utlevering av eierinformasjonen for over 20 000 norske IP-adresser, som rettighetshaverne mistenker har drevet med piratkopiering av seks navngitte filmer.

https://www.dagbladet.no/nyheter/tusenvis-av-norske-nettpirater-kan-bli-avslort/69528827

Film- og tv-bransjen har i alle år hevdet, og hevder fremdeles, at det pågår omfattende piratkopiering som medfører flere hundre millioner kroner i tapte inntekter hvert år. Interessen for rettssaken om utlevering av personopplysninger bak IP-adressene var svært stor blant våre lesere, noe som ga oss et signal om at mange kanskje lurte på om de selv var i fare for å bli avslørt. Vi bestemte oss for å se nærmere på temaet og spørsmålene ovenfor.

Etter å først ha undersøkt de siste fem års dommer for brudd på åndsverkloven, ble det tydelig at kun et svært begrenset antall personer er dømt for ulovlig fildeling i Norge. Dette ble nok en grunn til at vi ville undersøke bransjens påstander. For er virkelig ulovlig fildeling i Norge fremdeles så utbredt og et så stort problem som bransjen skal ha det til, selv etter lovendringen og tjenester som Netflix, Viaplay og HBO kom til landet?

Ressursbruk er en gjenganger når det kommer til **hvorfor** saker ikke blir prioritert etterforsket. Vi ønsket derfor også å undersøke **hvor ressurskrevende** det er å

finne ulovlige fildelere, både i form av arbeidstimer og økonomisk kostnad. Dette for å se om noe av forklaringen til at så få blir straffet ligger der.

Arbeidet med prosjektet har hovedsakelig gått over tre faser: datainnsamling, dataanalyse og det journalistiske arbeidet med kilder, intervjuer og skriving av artikler.

Dataene og journalistikken har vist at avstanden mellom bransjens syn på ulovlig fildeling og politiets prioritering av hverdagskriminaliteten er enorm. Mens bransjen selv bruker store summer i et forsøk på å avsløre og bekjempe nettpiratene, har politiet nesten ingen saker på bordet. De få som kommer inn, havner nederst på prioriteringslistene.

Oppstart og organisering

Etter at ideen om prosjektet ble lansert, satte en journalist og en utvikler i gang planleggingen og studerte mulighetene for innsamling av data. Vi visste at systemet for ulovlig fildeling i stor grad baserer seg på åpenhet. Dette innebærer at man til enhver tid kan se **hvilke** IP-adresser man deler en fil med, og **hvem** som deler filen med deg. Spørsmålet var derfor om vi kunne utnytte denne åpenheten til å avdekke **hvem** som deler filer uten at vi selv faktisk deltok i den ulovlige spredningen av materialet.

Det ble tidlig besluttet at det var ønskelig å overvåke fildelingsnettverket Bittorrent, da dette er et av de enkleste nettverkene å følge med på grunnet åpenheten som ligger til grunn for Bittorrent, mer om dette i neste kapittel.

Det ble også satt som mål at så mye informasjon om hva som er tilgjengelig via Bittorrent som mulig skulle anskaffes for å se hvor stor aktiviteten er i Norge, og på hvilke områder det er mest aktivitet. Vi valgte å se på områdene film, tv-serier, spill, programmer og e-bøker, med mistanke om at de to første ville stå for brorparten av aktiviteten.

Metoder

Tekniske metoder

Innledning

Innsamlingen ble utført ved å kategorisere såkalte info hasher på en rekke fildelingsnettsteder, samt søke etter hvilke IP-adresser som er aktive for hver av disse på DHT-nettverket (de tekniske begrepene er nærmere forklart i kommende avsnitt). Vi går her i litt næmere detalj rundt denne innsamlingen, samt videre bearbeiding av innsamlet data.

Verktøy

Alt av programvare som ble brukt i dette prosjektet, ble skrevet i programmeringsspråket Python. Dette inkluderer nettskrapere (system for å finne og laste ned innhold fra nettsteder, også kalt “crawlere”) og DHT-programmet som ble skrevet basert på et eksisterende Python-bibliotek. Underveis i innsamlingen ble data lagret i søkeprogrammet ElasticSearch for analyse, før det ble overført til en PostgreSQL-database hvor videre data-analyse ble utført. Geografisk presentasjon av dataene ble gjort med Google Maps.

Totalt ble det skrevet i overkant av 1400 linjer med kode i Python for dette prosjektet.

Bittorrent-nettverket

Bittorrent har vært i bruk i snart 20 år, og er et av de mest brukte systemene som brukes til piratvirksomhet i dag. Det finnes også flere andre løsninger (som Usenet, Direct Connect, Gnutella med flere), men ingen er like populære som Bittorrent. Alle fildelingsprogrammer har en viss grad av åpenhet for å finne andredeltakere å laste ned filer fra. Bittorrent har en rekke forskjellige måter å finne flere deltakere å laste ned filer fra.

Tidligere var det primært “trackere” som ble brukt, dette er sentraliserte tjenester som holder oversikt over alle som er involvert i deling eller nedlasting av gitte filer. Men etter hvert som antipirat-industrien, i form av interesseorganisasjoner og advokater på oppdrag fra filmbransjen med mål om å beskytte opphavsrett og åndsverk, gikk til søksmål mot operatørene av disse tjenestene, ble det utviklet en ny metode for å unngå en sentralisering av denne informasjonen. Det som nå har overtatt som primærmetode for å finne andre deltakere på, er det såkalte DHT-nettverket. Mer om dette i neste kapittel.

DHT-nettverket

DHT(Distributed Hash Table)-nettverket kan ses på som et eget nettverk som lever ved siden av bittorrent-nettverket. Dette nettverket holder på informasjon om hvem som laster ned og/eller deler hvilke torrent-filer (en torrent-fil inneholder en eller filer filer, f.eks filmer, TV-serier osv). En torrent-fil er på DHT-nettverket kjent gjennom en såkalt “infohash”(Unik ID), en infohash er resultatet av en såkalt “hashing” av en torrent-fil, noe som medfører at filen får en unik tekst på 40 tegn. Som eksempel “e84213a794f3ccd890382a54a64ca68b7e925433”.

Når et Bittorrent-program har DHT-nettverket aktivert og er involvert i en torrent-fil, det vil si at den enten laster opp, laster ned, eller bare har innholdet i en torrent-fil tilgjengelig for andre, skal den sende en melding til DHT nettverket minst hvert 15. minutt. Meldingen gir informasjon om infohash, IP-adresse og hvilken port andre nedlastere kan koble seg til. Denne informasjonen fordeles til en liten andel av deltakere i DHT-nettverket. Tilsvarende kan Bittorrent programmer som ønsker å

finne flere laste ned fra, sende en forespørsel om hvem som er involvert i en gitt infohash.

Her dukker det da i praksis opp to metoder å overvåke nettverket på. Den første er å sette opp et DHT-program som passivt logger alle som melder at de er aktive med en gitt infohash. Dette vil kreve mange virtuelle datamaskiner for å kunne plukke opp mest mulig, en må da også koble seg til de andre partene som er aktive for å finne ut filnavnet som tilhører hver infohash, mer om dette under presseetiske vurderinger nedenfor

Den andre metoden er da å gå inn på nettverket å spørre om hvem som er involvert med gitte infohasher. Denne metoden krever at en vet om infohash på forhånd, men vil gi betraktelig flere resultater med mye mindre ressurser. Dette er metoden vi valgte å gå for i dette prosjektet, slik at vi kunne få oversikt over ulovlig nedlasting.

Det finnes også en tredje metode som er aktivt bruk når det skal samles inn bevismateriale i fildelingssaker. Da går et program ut på nettverket og annonserer at den tilbyr en gitt infohash, som interesserte kan koble seg til. Det vil da loggføres hvor mye som deles på et helt annet nivå enn det vi har gjort i dette prosjektet. Denne metoden anså vi som for omfattende og inngripende for vårt prosjekt. Vi observerte derimot *slik aktivitet på DHT-nettverket fra norske IP-adresser.* Men da vi verken laster ned eller sitter på data kan ikke det ettergås videre.

Presseetiske vurderinger

Vi vurderte hvorvidt vi kunne bruke det vi fant på DHT-nettverket til å koble oss til de IP-adressene vi loggførte, da dette gitt oss oversikt over hvilke fildelingsprogrammer som brukes (f.eks hvor stor andel som er Popcorn Time brukere), hvor mye data som er delt, lastet ned osv. Vi kom til at vi i ikke ønsket å gjøre dette, da vi ikke ønsker å fremstå som for påtrengende eller potensielt fremstå som at vi aktivt prøver å laste ned materiale ulovlig. (Og dermed bli flagget hos piratjegere)

Fildelingsnettsteder

Det finnes en rekke nettsteder som tilbyr torrent-filer, den mest berømte av disse er “The Pirate Bay”, denne var derfor naturlig for oss å bruke som et nettsted hvor vi samler inn nødvendig data fra. Skjermbildet under viser hvordan en typisk fil blir presentert på det nettstedet.

Som nevnt i DHT-kapittelet har vi behov for infohasher, samt filnavnet og for enklere kategorisering; kategorien som filen er plassert i. En infohash er alltid unik, dette medfører at i dette eksemplet så vet vi at denne infohashen alltid vil være til en gitt versjon av filmen Deadpool 2, som er kategorisert som en HD-film. Vi vil da kunne gå på DHT-nettverket og spørre hvem som nå laster ned gitt infohash, og få vite om alle som nå laster ned denne versjonen av Deadpool 2.

Ettersom dette er et ganske greit eksempel på “scraping” av en nettside, skrev Tor Henning en nettskraper som besøkte The Pirate Bay ved gitte intervaller for å sjekke at vi alltid hadde alle de mest populære torrentene fra kategoriene vi var interessert i. Som nevnt over er infohashene alltid unike, så det er da en lett jobb å passe på at vi stadig får nye data lagret lokalt.

Etter at nettskraperen for The Pirate Bay var på plass og fungerte, ble prosessen repetert for seks andre nettsteder. Syv nettsteder ble overvåket i perioden prosjektet pågikk.

Innsamlingsfasen

Før vi igangsatte innsamlingsfasen hadde vi en periode hvor vi testet og fullførte DHT-programmet vår. Til slutt ble den konfigurert slik at den sjekket en tilfeldig infohash med noen sekunders mellomrom. Nye infohasher ble sjekket oftere, det samme ble infohasher hvor vi fant aktive norske IP-adresser. På denne måten kunne vi sjekke alle infohashene vi fant, men samtidig prioritere de vi tror vil gi oss “størst fangst”.

Programmet ble også satt opp med en kopi av en lokasjonsdatabase fra bedriften MaxMind. Denne databasen inneholder en oversikt over estimerte geografiske lokasjoner for IP-adresser. Kun trafikk som ble koblet mot norske IPer ble loggført, alt annet ble droppet.

Selve innsamlingsfasen gikk fra 16. Mars 2018 til og med 23. April 2018 Det ble i første omgang satt opp én virtuell datamaskin hos Google sin skytjeneste. Denne datamaskinen trålet torrent-nettstedene ved jevne mellomrom, samt utførte automatiserte søk på DHT-nettverket.

Etterhvert som innsamlingen av infohashene foregikk ble det klart at det ble for mange å overvåke for en enkelt datamaskin. Dette skyldes både at det krever en del data-ressurser å utføre søkene, og at vi ikke ønsker at en enkelt IP-adresse skal skille seg ut i mengden. Vi valgte derfor underveis i prosessen å sette opp flere virtuelle datamaskiner. Mot slutten av perioden hadde vi totalt 15 virtuelle datamaskiner som overvåket infohashene vi hadde samlet inn.

Da innsamlingsfasen var over hadde vi funnet og overvåket totalt 346 737 infohasher, innhentet over en periode på 39 dager.

DHT-programmet som kjørte på alle de virtuelle datamaskinene sendte alt som ble logget til søkeprogrammet ElasticSearch. Data som ble loggført var IP-adressen, infohash, filnavnet, tidspunkt, hostnavn, samt geolokalisering.

Vi overvåket søkeprogrammet i løpet av innsamlingen for se at alt kjørte som det skulle. Data eldre enn 24 timer ble overført til en kryptert maskin i redaksjonens lokaler, hvor det ble tatt sikkerhetskopier av dataene.

Det var ved starten av innsamlingen ikke bestemt hvor mye eller hvor lenge vi skulle la innsamlingen gå, dette ble en “se hvordan det går”-vurdering. Etter en ukes kjøring begynte vi å se at vi ville kunne nå 100 000 unike IP-adresser på rundt en måned.

Vi var også bevisst på utfordringen med anonymiseringstjenester, såkalte proxyer/VPN-tjenester, dette er tjenester som lar deg sende din egen nettverkstrafikk gjennom en annen IP-adresse, på den måten kan du skjule aktivitet og for utenforstående vil det da se ut som at din trafikk kommer fra et annet sted eller et helt annet land.

Ettersom vi ønsket å fjerne potensielle anonymiseringstjenester i ettertid, valgte vi å la overvåkingen samle inn i overkant 100 000 unike IP-adresser og stoppet først nå vi nådde i overkant av 107 000 unike IP-adresser.

Da innsamlingen var ferdig hadde vi loggført aktivitet på DHT-nettverket over syv millioner ganger fra de 107 000 IP-adressene.

Datarydding og geo-lokalisering

Etter innsamlingen var ferdig ble en kopi av dataene lastet inn i databaseprogrammet PostgreSQL for videre behandling. Det ble så satt i gang en kategorisering av alle IP-adressene. Vi valgte å sortere alle inn i kategoriene hjemmebruker, firma, og skole/kommune/fylke/offentlig.

Ettersom informasjon om hvem som bruker en IP-adresse i all hovedsak ikke er tilgjengelig for andre enn nettleverandørene selv, ble sorteringen løst ved hjelp av manuelle Whois-oppslag (Whois-oppslag gir indikasjoner på hva en IP-adresse brukes til, f.eks privat bruk, og i noen tilfeller, navnet på større bedrifter og

organisasjoner), kombinert med med et program som så på eierskap til IP-rekker (Nettleverandører får IP-rekker som de deler ut IP-adresser fra til sine kunder) samt eventuelle reverserte domenenavn knyttet mot IP-adressene. Størsteparten av IP-adressene kunne lett knyttes mot typisk hjemmebruk (blant de store internettleverandørene, bekreftet av Whois og/eller hostnavn)

Alle IP-adresser som ikke havnet i en av de forhåndsdefinerte kategoriene våre ble lagt i en egen kategori: anonymiseringstjeneste/ukjent. Det gjaldt også kjente anonymiseringstjenester, som for eksempel IP-adresser tilhørende anonymiseringstjenesten Tor. Disse IP-adressene ble sett bort fra i forbindelse med kartet og all statistikk.

Etter denne sorteringen hadde vi klart å kategorisere 101 000 IP-adresser som typiske privatadresser. 3000 IP-adresser tilhørende skoler, universiteter, kommuner, hoteller osv. Mens 778 IP-adresser kunne kobles mot mistenkte anonymiseringstjenester, og ble lagt vekk.

MaxMind oppdaterer sine posisjonsdatabaser ukentlig. I løpet av innsamlingsperioden vår hadde vi brukt en database, uten å oppdatere denne fortløpende. Vi valgte derfor å oppdatere geolokasjonene vi hadde samlet inn med oppdaterte posisjoner. Vi løste dette med å skrive et program som samkjørte loggtidspunkt og IP-adresse for å finne riktig versjon av databasen å sjekke mot.

Databasen vi bruker prøver å geolokalisere IP-adresser til nærmeste by/tettsted/kommune så godt det lar seg gjøre. Men her er vi også begrenset av det faktum at siden vi ikke har tilgang på hvem som sitter bak en IP-adresse, og må basere oss på det vi har. Mange av IP-adressene kunne ikke kategoriseres bedre enn at de er i Norge et sted, mens i andre tilfeller visste vi (basert på Whois data) at data ble plassert korrekt. I praksis ender vi opp med geoposisjonering som kan gi oss cirka-oversikt over hvordan fordelingen av ulovlig nedlasting er i Norge.

(Første variant av kartet med alle unike steder plottet inn)

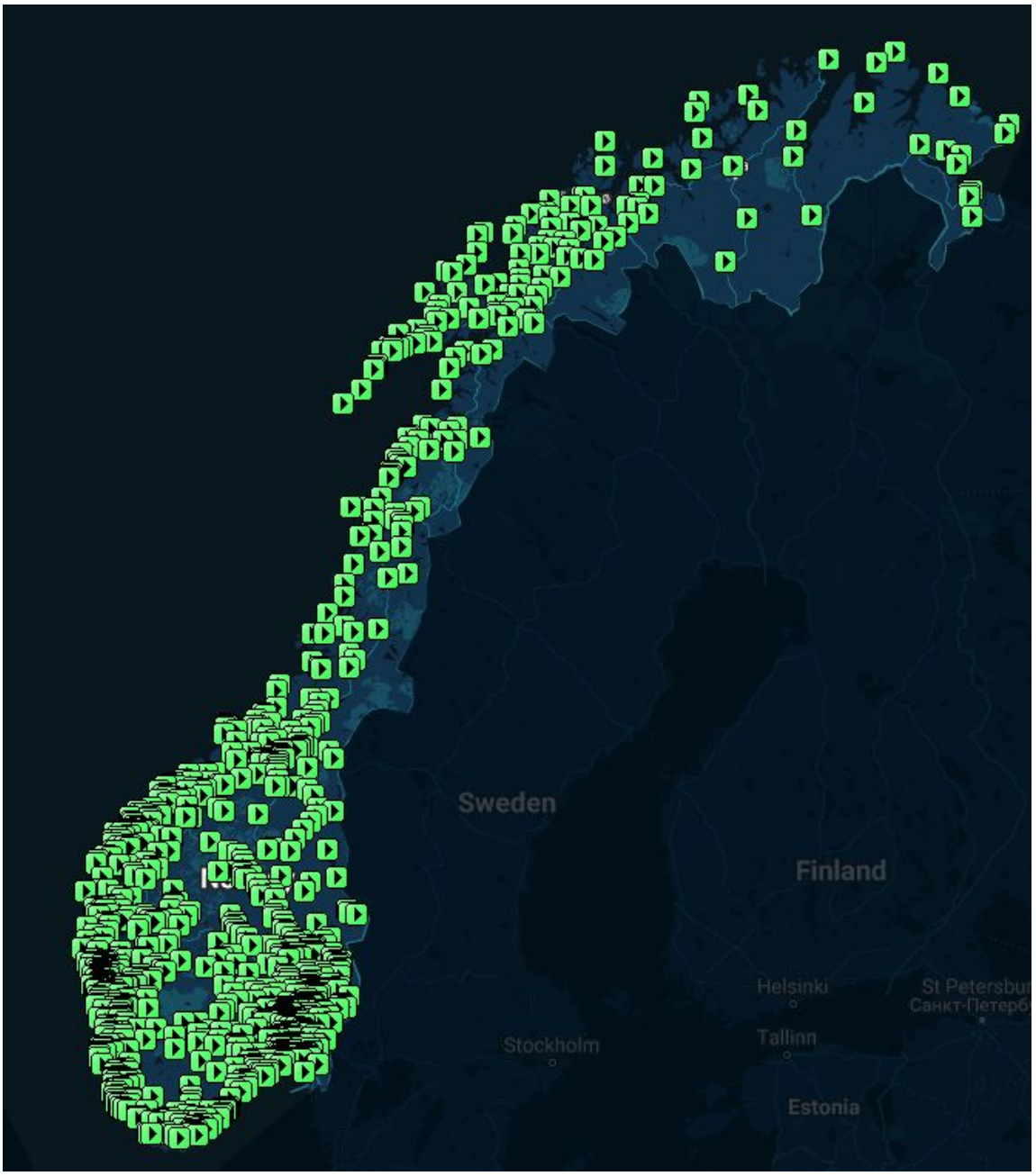
Kartet

For å visualisere at piratvirksomhet er noe som foregår overalt i landet, var det ønskelig å presentere dette i et kart. Dataene vi sitter på, ga oss en fin mulighet til det. Totalt hadde vi en liste over antall unike IP-adresser lokalisert på 1052 forskjellige steder i Norge.

Ved å plassere funnene geografisk, oppnådde vi særlig tre ønskelige resultater:

- Vi fikk svar på ett av våre opprinnelige spørsmål: **Hvor skjer** ulovlig fildeling?
- Vi avdekket at det verken er et by- eller bygdefenomen.
- Vi ga leserne muligheten til å gå inn på sin by/tettsted/bygd og se hvor mange fildelere vi hadde sporet opp der de bor eller der de ville sjekke selv.

Kartet ble bygget opp med vanlige markører i produktet Google Maps. Vi utarbeidet også et egendefinert tema og ekstra lag for å utheve Norge på kartet.



(Endelig kart)

Presseetiske vurderinger

Vi ønsket ikke å henge ut privatpersoner for ulovlig nedlasting med dette prosjektet. Alle steder som hadde færre enn tre nedlastere ble derfor manuelt sjekket for å se at de ikke ble lokalisert til et sted med såpass få hus at det kunne få rykter til å gå. I de tilfellene det ble funnet ble stedene fjernet fra kartet.

Etter publisering fikk vi også et par kommentarer på kartet kunne zoomes inn for mye, slik at enkelte steder kunne fremstå feil (en markør satt i en fjord, f.eks), eller som at vi hadde funnet et spesifikt hus, og poenget med at vi viste antallet IP-adresser per sted, kom da ikke godt nok frem. Vi valgte da å begrense zoom-funksjonaliteten på et nivå som gjør at kun får et oversiktsbilde.

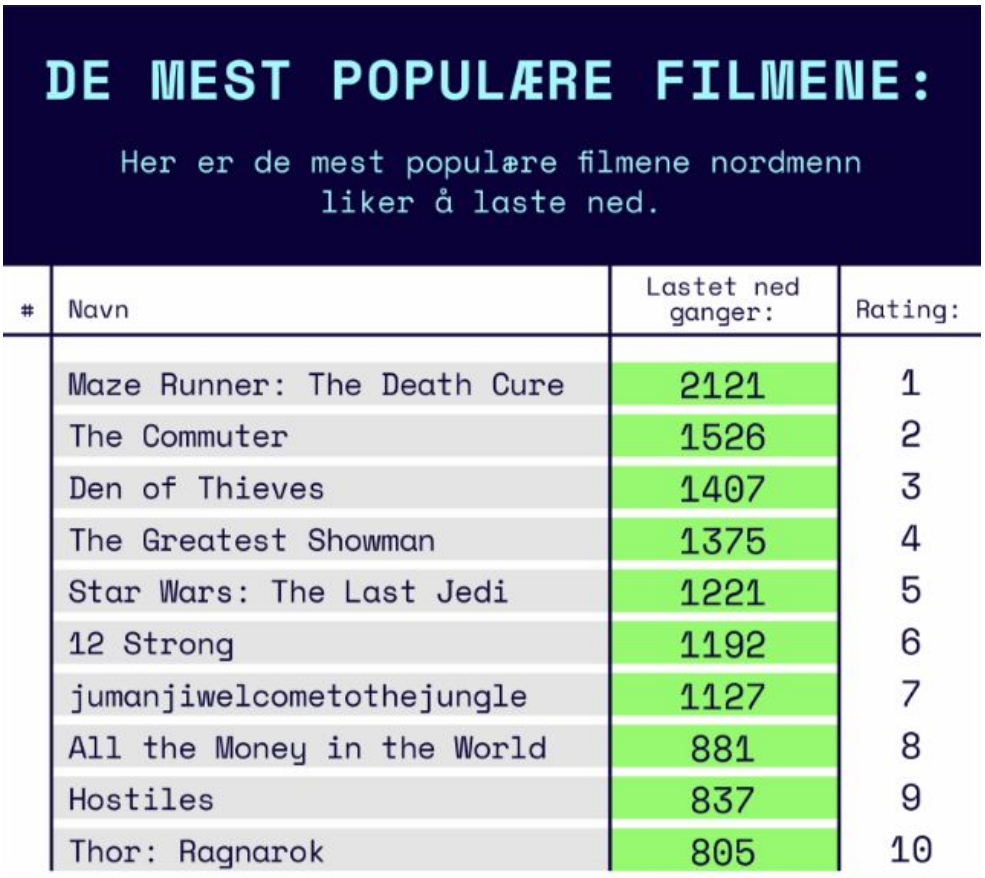
Topplister

For TV-serier og filmer ønsket vi å vise hvilke som var mest populære i den perioden hvor vi samlet inn data. Å finne ut hva som er mest etterspurt er som regel en sak som er rett frem. I en perfekt verden kunne vi bare sjekket alle unike IP-adresser som har sett filmen “The Commuter”. Så lett er det ikke når det gjelder piratkopiert innhold. En hver versjon av filmen kommer nemlig med sitt eget filnavn, i tillegg vil forskjellige grupper som lanserer filmene på fildelingsnettverk ha med sine navn i filnavnene.

For “The Commuter” fant vi totalt 227 forskjellige infohasher med 197 forskjellige filnavn, noen eksempler er:

- The.Commuter.2018.2160p.BluRay.REMUX.HEVC.DTS-HD.MA.TrueHD.7.1.Atmos-FGT
- The.Commuter.2018.720p.BluRay.x264-DRONES[EtHD]
- The.Commuter.2018.V2.720p.HC.HDRip.X264.AC3-EVO
- The Commuter 2018 720p NEW HD-TS X264-CPG

Løsningen her ble å bruke programmet Jupyter Notebook til å lage et system som vi kjørte alle filnavn gjennom så vi fikk normalisert de. Programmet består i praksis av en rekke regulære uttrykk som fjerner alle kategoriseringer, gruppenavn, spesialtegn og så videre. Til slutt står vi da igjen med “The Commuter 2018”. I enkelte tilfeller stod vi igjen med mellom én til fem forskjellige filnavn per fil. Men vi var da nede i såpass få filer at vi kunne gjøre en manuell bekreftelse for å se at vi hadde funnet antall unike nedlastinger per film/serie-tittel. (IP-adresser vi klassifiserte som anonymiseringstjenester ble ikke tatt med i disse tallene)



DE MEST POPULÆRE FILMENE:

Her er de mest populære filmene nordmenn liker å laste ned.

#	Navn	Lastet ned ganger:	Rating:
	Maze Runner: The Death Cure	2121	1
	The Commuter	1526	2
	Den of Thieves	1407	3
	The Greatest Showman	1375	4
	Star Wars: The Last Jedi	1221	5
	12 Strong	1192	6
	jumanjiwelcometothejungle	1127	7
	All the Money in the World	881	8
	Hostiles	837	9
	Thor: Ragnarok	805	10

(Den ferdige topplisten for filmer)

Journalistikken

Med dataene i boks, startet vi selv jakten på en ulovlig fildeler som kunne figurere som eksempel i vår reportasjeserie. Til tross for at vi nå visste at dette var svært utbredt, tok det tid før vi fikk kontakt med noen som ville stille opp. Løsningen ble til slutt å legge ut en forespørsel på et nettforum (Freakforum), hvor vi visste at temaet er hyppig diskutert, og at sjansen for at noen ville melde interesse var til stede.

Målet var å få kontakt med en person som hadde drevet med fildeling i lang tid. Hovedårsaken til dette, var at vi ikke bare ønsket å belyse våre funn, men også få en stemme som kunne si mer om de spørsmålene vi hadde innledningsvis:

- Hvorfor skjer ulovlig fildeling fremdeles, til tross for de lovlige tjenestene?
- Hvem driver med deling av piratkopiert materiale?
- Hva deles?
- Hva må til for at omfanget av ulovlig fildeling skal reduseres?

Vi sørget for at personer som ønsket å ta kontakt anonymt, kunne gjøre dette kryptert.

Vi fikk flere henvendelser, men det var først etter et par dager at han som til slutt ble vår fildelings-case tok kontakt. Dette var en mann i slutten av 20-årene som hadde drevet med omfattende ulovlig fildeling siden starten på 2000-tallet. Han sa seg villig til å la seg intervjue, så lenge han fikk forbli anonym.

Etter innledende intervju via telefon og mail, ble det klart at han hadde reflektert mye rundt spørsmålene vi ønsket svar på. Vi dro til Aust-Agder for å gjennomføre et grundig intervju med vedkommende.

Presseetiske vurderinger
Presseetikken ble hele veien vurdert, og til tross for at vi allerede visste at politiet avslører svært få nettpirater, var det viktig for vår case at identifisering ikke var mulig gjennom intervju, bilde eller video. Både vi og han selv har bidratt til og godkjent anonymiseringen og bruken av tekst og bilder før publisering.

Den største motpolen til nettpiratene er film- og tv-bransjen selv, som i hele Norden driver en offensiv jakt på personer som driver ulovlig fildeling. I spissen for dette, finner man det danske advokatfirmaet Njord lawfirm, som flere filmselskaper har brukt. Firmaet har kjørt flere hundre rettssaker mot fildelere i Danmark, og har sendt ut totalt 150 000 økonomiske krav til nettpirater i Danmark, Finland og Sverige. De var også den som representerte bransjen da det ble krevd utlevering av personinformasjonen bak mer enn 20 000 norske IP-adresser i Oslo tingrett tidligere i år, men selskapet har så langt ikke hatt noen omfattende aktivitet i Norge.

Advokatselskapet ble intervjuet i forbindelse med den innledningsvis nevnte saken fra februar, og sa seg villige til å møte oss i København for å fortelle om sin side av saken knyttet til vår kartlegging. Dagen etter at vi hadde møtt vår nedlaster-case, dro vi derfor til Danmark for å intervjue advokaten der.

Underveis i intervjuet presenterte vi også datafunnene vi selv hadde gjort og argumentene vårt nettpirat-case mente var årsaken til at det fremdeles pågår ulovlig fildeling. Advokaten anså funnene og kartleggingen som interessant. Han var likevel ikke overrasket over omfanget, ut ifra erfaringene de har fra andre nordiske land.

I Norge finnes det en rekke filmselskaper. Vi valgte å gå til bransjeorganisasjonen Norsk Videogramforening, da vi skulle ha en stemme fra de som er skadelidende på grunn av den ulovlige fildelingen. Foreningen har i en årrekke fått statistikk for utbredelsen av ulovlig fildeling i Norge fra et svensk medieanalysebyrå. Tallene deres baserer seg på spørreundersøkelser..

Vi fikk tilgang til oppdaterte tall, som viste at hver sjuende film og tv-serie som ses i Norge er lastet ned ulovlig. Vi fikk også et estimat på hvor mye bransjen mener de taper årlig økonomisk på grunn av ulovlig fildeling.

Tallene for økonomisk tap og omfang av ulovlig fildeling ble gitt fra et interesseorgan for filmbransjen. Vi forsikret oss derfor at statistikken var basert på data fra et representativt utvalg og sørget for en begrunnelse for hva som lå bak beregningen av det økonomiske tapet.

Siden vi allerede visste at det var svært få som hadde blitt stevnet for retten og dømt for ulovlig fildeling i Norge, selv etter Piratloven trådte i kraft, var det naturlig å konfrontere politiet med våre funn. I tillegg ville vi finne ut hvor høyt slike lovbrudd prioriteres.

Vi tok kontakt med flere av politidistriktene, og fikk tilbakemelding fra henholdsvis Oslo, Sør-Vest og Agder. Disse opplyste at det er lokalt politi som etterforsker slike saker og at ingen etterforskning blir satt i gang før en eventuell anmeldelse foreligger.

Vi fikk også opplyst at det hos de tre politidistriktene kun hadde vært en håndfull tilfeller av saker totalt de siste årene. Hos Agder politidistrikt fikk vi også vite at de så langt i år hadde fått én anmodning om bistand fra lokalt politi i en fildelingssak. Denne ble avslått på grunn av manglende ressurser. Sør-Vest opplyste at saker som involverer ulovlig fildeling sjelden eller aldri havner på deres bord, og er nederst på prioriteringslistene.

Til tross for mangel på ressurser, er det ifølge Sør-Vest politidistrikt ikke faglig kunnskap som gjør at nettpirater ikke blir tatt eller prioritert etterforsket i Norge. Ressursene fører imidlertid til at kompetansen innen fildeling blir brukt til å avsløre spredning av overgrepsmateriale, og at dette skjer i så stort omfang at man ikke har kapasitet utover det.

Siden vi via det danske advokatfirmaet allerede hadde løftet blikket til et nordisk nivå, ville vi undersøke hvordan politiet jobbet i andre land. Vi valgte oss ut Sverige, og kom etter hvert i kontakt med riktig person der.

Det viste seg at Sverige, i motsetning til Norge, hadde et offensivt arbeid og en egen gruppe etterforskere som jobber med saker som involverer fildeling. Dette hadde blant annet ført til 40 saker med nettpirater de siste 18 månedene.

Etterspill


Fjell-Ljom

Matfag kommer i høst

Legg kul-turen til fjells

ORIGINAL RØROSAVISEN

Nettpirat-hovedstaden finner vi på Røros

Opphørssalg hos opphørssalgsbutikk

Men de fleste i Kjerkgata driver godt

Trenger blåbær til perlende drikker

VARETAXI

Jonny Vollan

Dagbladets avsløringer har, til tross for den relativt ferske lovendringen fra 2013, ikke ført til store politiske eller juridiske reaksjoner. Avsløringene har likevel medført at temaet har fått fokus og satt dagsorden i enkelte lokalaviser i landet.

Vi har i tillegg til å aktualisere og vise omfanget av ulovlig fildeling, fått vist hvordan folk anser faren for å bli tatt for dette. Ved små, enkle tekniske grep kan man sørge for å skjule seg bak anonymiseringstjenester som vil gjøre faren for å bli tatt nærmest lik null. Til tross for dette, velger titusenvis av nordmenn å laste ned film og tv-serier ulovlig, helt åpenlyst.

Dette forteller oss at norske nettpirater mener faren for å bli tatt for denne hverdagskriminaliteten, fem år etter at det ble fastslått at det er straffbart, er svært liten.

Til slutt

Arbeidet med Dagbladets artikkelserie om nettpiratene startet uten noen store tips, men med en hypotese om at ulovlig fildeling er en form for kriminalitet som "alle" driver med, men ingen blir tatt for. Målet var derfor å finne ut om inntrykket vårt stemte, ved å dokumentere det som skjer med konkrete tall. Vi ville videre sjekke om nettpiratene i dag har noen reell risiko for å bli tatt.

Prosjektet bekreftet flere av hypotesene våre, men også ga oss en oppvekker med tanke på hvor lett det faktisk var å spore opp IP-adressene til nettpiratene og hvor omfattende ulovlig fildeling fremdeles er. Vi håper metodene våre kan gi inspirasjon og brukes til lignende prosjekter i Norge og andre land, i tillegg til at det har gitt både lesere og de som forvalter loven innblikk i omfanget av og hvor lett man faktisk kan kartlegge denne hverdagskriminaliteten.

Oppsummering av prosjektet:

- Vi tallfestet hvor omfattende ulovlig nedlasting av film- og tv-serier er i Norge.
- Vi dokumenterte den geografiske spredning av ulovlig fildeling, som viser at dette fremdeles er en utbredt kriminalitet som ikke er geografisk avgrenset. Vi tegnet også norgeskartet over fildeling.
- Vi dokumentere hva som ble lastet ned hvor mye (mest/minst populært).
- Vi dokumenterte at det i prinsippet er "lett" og billig å kartlegge ulovlig nedlasting, fordi systemet er veldig åpent. Dette kunne vært benyttet av myndighetene - dersom det var ønske om å kontrollere og straffe nettpirater.
- Vi brukte vårt datamateriale til å problematisere de juridiske rammene og samfunnets reaksjoner på fenomenet ulovlig fildeling: Stortinget har vedtatt at det er et brudd på norsk lov. Spill- og TV-bransjen taper store beløp på at åndsverk distribueres gratis. Samtidig er fenomenet svært utbredt, lovforbudet har liten legitimitet og politiet/myndighetene bruker ikke ressurser på å straffeforfølge dem som stjeler åndsverk på nettet. Sjansen for å bli tatt for denne hverdagskriminaliteten er derfor svært liten.

Linker til publiserte saker i prosjektet

https://www.dagbladet.no/nyheter/106-607-nettpirater-her-bor-de-dette-laster-de-ned-slik-vil-filmbransjen-ta-dem/69897233#_ga=2.176604005.110016481.1532953840-637052164.1517849075

https://www.dagbladet.no/nyheter/dagbladet-avslorer-106-607-nettpirater---bransjen-taper-en-halv-milliard-i-aret/69897331

https://www.dagbladet.no/nyheter/derfor-nekter-teleselskapene-a-avslore-norske-nettpirater/70047137

https://www.dagbladet.no/nyheter/slik-jakter-svensk-politi-pa-ulovlige-fildelere/70050300

https://www.dagbladet.no/nyheter/slakter-filmbransjen-og-danske-advokaters-jakt-pa-norske-nettpirater/70063296

https://www.dagbladet.no/kultur/umoden-piratjakt/70051673