METODERAPPORT SKUP 2018

Jakten på «Edderkoppen»

Journalister: **Henrik Lied, Trude Furuly** og **Truls Antonsen** (fotograf)
Utviklere: **Johannes Odland** og **Glen Imrie**

NRK Bjørnstjerne Bjørnsons plass 1, 0340 Oslo

1. Innledning

Maiken Skoie Brustad er egentlig ganske fornøyd med seg selv og livet sitt. Hun er 23 år, har akkurat flyttet til London med kjæresten og nettopp fått ny jobb som personlig trener. Hun småprater med personalet i en av metropolens vintagebutikker da det plinger i mobilen. Facebook-meldingen får verden til å rase sammen. Noen har funnet nakenbilder av henne på et nettforum.

Flere år senere skulle det vise seg at Maiken ble ett av de mange ofrene til mannen som NRK har valgt å kalle «Edderkoppen». Fra datamaskinen trakasserte og rundlurte han en lang rekke norske kvinner i over seks år. Under dekke av flere titalls falske identiteter, og med ganske elementære datakunnskaper, kontaktet han flere hundre intetanende kvinner.

Politiet klarte ikke å finne mannen, til tross for at de mottok anmeldelser og tips til ulike politidistrikt. Gjennom utstrakt bruk av domenesøk, innsynsprosesser, systematisering og kildearbeid, lyktes NRK med å avdekke sammenhengen mellom flere av sakene som lå henlagt hos politiet. NRK fant også mannen som stod bak.

2. Slik startet det

I november 2017 skulle NRK Nyheter lage en sak om ulovlig spredning av nakenbilder. Temaet fikk mye oppmerksomhet i media etter #Metoo og sakene om håndballspiller Nora Mørk. Journalist Trude Furuly forhørte seg med folk i sin omgangskrets om de visste om noen som hadde fått private nakenbilder spredt på nett. Slik dukket navnet Maiken Skoie Brustad opp. Det lå mange meget intime bilder av Maiken på nett, og journalisten tok kontakt med henne. Maiken fortalte en hjerteskjærende historie.

Da Maiken i 2016 ble gjort oppmerksom på at hennes private bilder lå på nett, kontaktet hun den norske veiledningstjenesten Slettmeg.no på e-post. På kvelden samme dag fikk Maiken en e-post som snudde livet på hodet:

> **Fra:** Oscar Persson
> **Til:** Maiken
> **Sendt:** 19.08.2016, 23:11
>
> ---
>
> Hei
>
> Jeg jobber i den svenske delen av det statlige foretaket www.slettmeg.no (NorSIS) som jobber med å slette uønskede bilder av mennesker på internett. På flere nettsteder har vi funnet svært mange nakenbilder av deg.
>
> Vennligst ta kontakt med oss snarest, for fremgangsmåte for å få disse slettet (kostnadsfritt) og eventuelt bistand til politianmeldelse. Dette forutsatt at det ikke er deg selv som har lastet disse opp.
>
> Oscar Persson
> Seniorkonsulent

Maiken var desperat etter hjelp. Hun hadde ingen anelse om at hun gikk i fella. Svensk Slettmeg.no eksisterer ikke.

«Oscar Persson» kommuniserte med Maiken på e-post og via en falsk profil på Facebook i flere uker. Han sa han jobbet med å fjerne nakenbildene fra nett. Etterhvert flyttet han samtalen over på Hipchat, som er en kryptert kommunikasjonsplattform. Han oppga at han hadde dyktige samarbeidspartnere, blant annet en datakonsulent i USA. Alt dette var usant, men Maiken fikk umiddelbart tillit til «Oscar».

Han påstod at han var i ferd med å spore opp den som stod bak spredningen av nakenbildene, og jobbet med en politianmeldelse Maiken kunne levere. «Oscar» opplyste også at han hadde funnet en video av henne hvor hun ble voldtatt mens hun var veldig beruset. Hun trodde først at dette var sant. Dette var en stor belastning, men hun har i ettertid blitt helt sikker på at dette ikke har skjedd.

I en e-post skrev «Oscar»: *«Hvem utenom dine sexpartnere har kjennskap til sexlivet ditt, og har du noen gang hatt sex på steder hvor andre kan ha sett / fanget dett opp, kan du i såfall bekrefte for meg hvor og når.»*

I en annen e-post skrev han: *«Pust helt rolig Maiken. Jeg kan informere deg om at jeg allerede har begynt å identifisere mennesker som laster ned bilder [..].»*

Etter flere ukers kontakt avtalte de å møtes på Torp flyplass for å forberede anmeldelse og deretter rettssak mot den som hadde stått bak bildespredningen. Maiken og moren møtte opp til avtalt tid. Men «Oscar» dukket aldri opp. Først denne dagen forstod Maiken at hun hadde blitt lurt. Hun brøt all kontakt med mannen.

Etter hendelsen på Torp flyplass mottok Maiken en rekke trakasserende meldinger på e-post og sosiale medier. De kom fra en rekke anonyme avsendere. Maiken mistenkte med en gang at «Oscar» stod bak. Maiken politianmeldte bildespredningen og «Oscar», men hadde ingen anelse om hvem han var.

Maiken overleverte korrespondansen til NRK. Etter å ha lest gjennom materialet, slo det oss hvor mye tid og krefter han hadde brukt på Maiken.

Kunne Maiken være bare ett av flere ofre?

Hvem var denne såkalte «Oscar Persson», og hvorfor gjorde han dette?

2.1 Hypoteser

Vi utarbeidet følgende hypotese:

- Vi mistenkte at personen bak e-posten hadde drevet med nett-trakassering over lengre tid. *Hadde han flere ofre?*

Vi visste at e-posten fra Slettamig.se kom bare timer etter at Maiken hadde kontaktet norske Slettmeg.no på e-post. Selv om dette kunne være en ren tilfeldighet, vurderte vi også følgende:

- Vedkommende har hatt tilgang til Maikens datamaskin eller e-posten til Slettmeg.no
- *Dersom dette stemte, kunne det også bety at «Oscar» hadde hacket Maiken eller selv vært med på å spre bildene hennes – før han tilbød seg å hjelpe med å fjerne dem?*

Dette var utgangshypotesene, og vi bestemte oss for å prioritere arbeidet med saken. Hypotesene skulle justeres flere ganger underveis.

3. Derfor var saken viktig

Saker som omhandler ulovlig spredning av bilder, trusler og trakassering på nett, får lav prioritet hos politiet. Ofte på grunn av allerede store saksmengder, men også på grunn av manglende kompetanse. Gjennom partsinnsyn fikk vi et innblikk i hvordan politiet etterforsker denne typen saker. Etterforskningen baserte seg på ganske grunnleggende bruk av Google og intervjuer med noen av de berørte partene.

Den psykiske belastningen for de som opplever trusler, trakassering og ulovlig spredning av intime bilder på nett, er ofte enorm. Et fåtall av ofrene orker å snakke høyt om det eller stå frem i media. Maiken er en av de få.

Hun klarte i perioder ikke å gå på jobb, og gikk fast til psykolog etter at hun ble utsatt for «Oscars» trakassering. Han fortsatte å ta kontakt gjennom andre kanaler på nett. Hun anmeldte hendelsen til politiet. På grunn av mangel på bevis, ble saken henlagt etter kort tid.

Dette er et problem. En stadig større del av dagens kriminalitet foregår i den digitale sfære. Det finnes et eksempel fra Norge i 2017, hvor en ung mann tok livet sitt etter å ha blitt presset for penger av kriminelle som hadde manipulert han til å utføre seksuelle handlinger på nett.

Da henleggelsen kom, følte Maiken seg alene og hjelpeløs. To år senere satt hun fortsatt uten svar. Det var flere spor å følge, og om noen ville forsøke å nøste i «Oscars» identitet, ville det bety mye for henne. Samtidig kunne en sak kanskje få betydning for flere – *tenk om personen bak aliaset «Oscar Persson» lurte mange andre?*

Vi bestemte oss for at dette ikke bare skulle bli en historie om Maiken – vi ville også finne gjerningsmannen.

Den digitale jakten på å avsløre «Oscar» ble krevende, og på mange måter en digital kompetansekrig mellom han og oss. Han hadde gjort mye for å skjule sporene sine.

4. Slik organiserte vi oss

Journalistene Henrik Lied og Trude Furuly, og fotograf Truls Antonsen jobbet med saken sammen med utviklerne Johannes Odland og Glen Imrie.

Fra januar 2018 ble noen av de involverte i perioder tatt ut av vanlige arbeidsoppgaver for å jobbe med prosjektet. I tiden før publisering ble illustratør Marco Vaglieri, fotograf Patrick da Silva Sæther, skrivecoach Mads Nyborg Støstad og nyhetsjournalist Camilla Wernersen koblet på.

5. Slik gjorde vi det

5.1 Fase 1 – Kartlegging av «Oscars» aktivitet

Maiken hadde tatt vare på mye av kommunikasjonen med «Oscar». Hun hadde en stor mengde e-poster og skjermkopier av facebook-samtaler. Dette, sammen med anmeldelsen hun selv hadde levert til politiet, ga oss et godt innblikk i saken.

Vi plottet alle hendelser (e-postutvekslinger, Facebook-meldinger, o.l) inn i en tidslinje i Excel, med dato og klokkeslett. I lange intervjuer med Maiken spurte vi om detaljer som manglet og fikk svar på ubesvarte spørsmål. Vi snakket også med Maikens mor på telefon for ytterligere informasjon og detaljer.

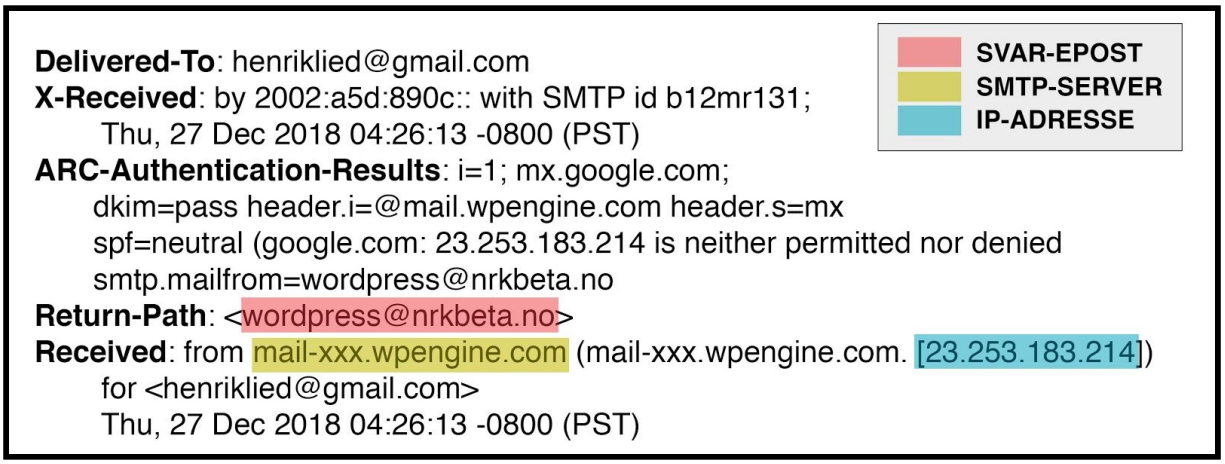
Sporene på Maikens PC

Maiken ga oss tillatelse til å gjennomsøke PC-en hennes. Dersom «Oscar» hadde hatt tilgang til Maikens maskin eller e-postkonto, kunne han ha lagt igjen spor flere steder, som for eksempel i metadata eller i forbindelse med kompromitteringforsøk. Slike detaljer kunne ligge igjen på Maikens datamaskin. Datajournalist Henrik Lied gjennomsøkte maskinen etter spor. Han lette da etter følgende:

1. Metadata i e-poster
I en e-post ligger det ofte mer informasjon enn det som er synlig for det blotte øyet. Dette kalles e-postens «header». I headeren kan det ligge informasjon som kan si noe om avsender, som for eksempel hvilken nettadresse e-posten er sendt fra. Måten man får opp e-postheadere varierer fra e-postsystem til e-postsystem. I Gmail blir headeren synlig ved å trykke på symbolet med tre prikker oppe i høyre hjørne, og velge “vis originalen”.

Da vi gikk gjennom headerene på e-poster fra «Oscar» fant vi en referanse til en norsk domeneleverandør. Det sannsynliggjorde at personen som stod bak domenet Slettamig.se hadde registrert det i Norge. Dette kunne gjøre det enklere for oss å finne identiteten til eieren.

Illustrasjonen nedenfor er et eksempel som viser hvordan e-postheadere ser ut. Viktige detaljer er markert med farger:



I svindelforsøk er ofte "**svar-eposten**" satt til noe annet enn e-postadressen meldingen ble sendt fra. For eksempel, kan man få en e-post fra navn.navnesen@microsoft.com, mens svar-epostadressen er satt til navn.navnesen@eksempel.com. Dette er informasjon som ofte ikke er så tydelig vist i e-postklienten, men som man enkelt kan se i e-postheadere. Outlook, Gmail og Hotmail er eksempler på ulike e-postklienter. Slik kan man finne ut om en e-post kommer fra en annen avsender enn den som er synlig i forhåndsvisningen.

En **SMTP-server** forteller oss hvilken e-postserver som e-posten har gått gjennom før den endte opp hos mottakeren. Vi så at e-posten var sendt fra en norsk SMTP-server. I teorien kunne dette gjøre det mulig for oss å finne mer informasjon om personen bak e-posten.

Også **IP-adresser** er ofte inkludert i e-postheaderne. Dette kan enten være IP-adressen til **SMTP-serveren**, men i mange tilfeller også IP-adressen til datamaskinen som sendte e-posten. Ved å sjekke IP opp mot geografiske registere, som for eksempel https://dazzlepod.com/ip/, kan man få en viss indikasjon på hvor i verden den aktuelle IP-en befinner seg. Merk at denne form for søk ofte har store feilmarginer, men at det vanligvis er nøyaktig ned til landnivå. Ved å bruke denne metoden, fant vi ut at flere av e-postene fra «Oscar» var sendt via norske servere. Så langt tydet våre funn på at han var bosatt i Norge.

2. Elementer i e-poster som kunne inneholde informasjon

Hvis «Oscar» hadde sendt bilder eller filer til Maiken i deres samtaler, kunne de inneholde metadata, som for eksempel når bildene ble tatt, hvilket kamera som ble brukt eller geografiske koordinater. Slik informasjon kan ligge i EXIF-metadata i bildene.

Vi fant flere filer i korrespondansen, og kjørte disse gjennom verktøyet ExifTool (http://owl.phy.queensu.ca/~phil/exiftool/) for å analysere filenes metadata. Vi sjekket filene, men dessverre måtte vi konstatere at all personlig identifiserbar informasjon var fjernet. Denne metoden ble dessverre bom.

3. Tegn på at brukerkontoene var forsøkt kompromittert
Men vi ga ikke opp. Vi ville også undersøke om noen av Maikens kontoer var forsøkt kompromittert (forsøkt hacket). *Hadde noen av kontoene til Maiken (PC, e-post, Facebook-bruker eller andre nettkontoer) blitt kompromittert, og var det derfor bildene av henne hadde lekket? Kunne også «Oscar» ha vært den som delte de intime bildene av Maiken?*

Dersom utenforstående prøver å komme seg inn på brukerkontoer på nett, kan dette bli loggført som mislykkede innloggingsforsøk. En gjennomgang av loggen til Maikens e-postkonto viste flere slike mislykkede forsøk, med IP-adresser fra Russland og land i Asia.

Vi sjekket de aktuelle IP-adressene opp mot servere i Tor-nettverket ved hjelp av tjenesten Tor ExoneraTor (https://metrics.torproject.org/exonerator.html). Tor-nettverket brukes ofte av aktører som er ute etter å skjule sine digitale spor, og er flittig brukt av kriminelle.

Vi sjekket også om Maikens brukerkontoer hadde blitt kompromittert. Til dette brukte vi nettstedet «Have I been pwned» (https://haveibeenpwned.com/). Her la vi inn e-postadressene til Maiken, og fant ut at hennes brukerdata hadde blitt lekket i fire lekkasjer.

For å finne ut hvilke av Maikens passord som var lekket, lastet vi ned databasen «BreachCompilation», som inneholder 1.4 milliarder brukernavn- og passordkombinasjoner. Vi bygget så et enkelt verktøy i programmeringsspråket Python for å sjekke om noen av Maikens e-postkontoer var tilstede i denne databasen. Databasen vi lastet ned bestod av tusenvis av mindre tekstfiler, hvor hver linje var en sammensetning av «e-postadresse:passord». Hvis man skulle søkt på disse filene manuelt hver gang, ville det tatt over en time å gjøre ett enkelt søk.

Derfor bygget vi verktøyet i Python, som leste gjennom alle linjene i alle filene på én gang. Verktøyet kunne da lage et søkbart objekt, som kunne ta imot både fullstendige og ufullstendige e-postadresser og passord, og gi oss resultatet på millisekunder. Vi fikk flere treff, men passordene var gamle og ikke lenger i bruk.

Selv om denne metoden ikke førte oss videre i arbeidet, er det en nyttig metode man bør bruke når man undersøker digitale spor.

Etter undersøkelsene på Maikens maskin hadde vi ikke funnet noe som kunne påvise at «Oscar» kontrollerte Maikens e-post, eller at han sto bak selve bildedelingen. En rekke metoder vi visste var gode å bruke, hadde til nå ikke ført frem.

Men vi ville ikke gi opp. Vi hadde fortsatt et kort igjen på hånda: E-postadressen oscar@slettamig.se. Denne e-postadressen hadde «Oscar» brukt da han kontaktet Maiken første gang.

Nye forsøk

E-postadressen sluttet på .se, og tilhørte derfor et svensk domene. Hvis personen som sendte e-postene var den samme personen som hadde opprettet domenet, måtte vår neste oppgave bli å finne identiteten til den som hadde registrert domenet.

Når et domene opprettes, registreres dato for opprettelse sammen med kontaktinformasjon til eier, og hvilken registrar som er ansvarlig for domenet. Denne informasjonen kan man finne med ulike domenesøk på nett (f.eks. https://who.is/ eller http://whois.domaintools.com/). Tjenestene lar deg søke opp registreringsinformasjon knyttet til et domene. DomainTools har også historiske data for hvem som har vært eiere av et domene over tid.

Søket på «Slettamig.se» ga oss begrenset med informasjon fordi kontaktinformasjonen var anonymisert. To viktige opplysninger var likevel synlige: At domenet ble opprettet i 2015, og at det var koblet til en norsk server. At det svenske domenet var tilknyttet en norsk server, var en god indikasjon på at domenet var registrert via en norsk leverandør.

Vi mistenkte at domenet var opprettet av «Oscar», slik at han kunne fremstå som en representant for Slettmeg.no på e-post.

Slettmeg.no og Slettamig.se

Vi hadde tidlig i arbeidet funnet en nettartikkel hvor NorSIS, Norsk senter for informasjonssikring, (som eier Slettmeg.no) i 2016 hadde advart mot en falsk utgave av Slettmeg.no. Artikkelen var publisert i samme tidsrom som Maiken hadde blitt lurt. Saken inneholdt også informasjon som viste med all tydelighet at det var gode grunner for å intensivere jakten på «Oscar Persson»: NorSIS skrev at flere jenter hadde blitt kontaktet av en med det samme navnet.

Innsyn hos IIS

Fordi mye informasjon var anonymisert i domenesøket, måtte vi forsøke en annen metode for å få tak i mer informasjon om domenet. Vi kontaktet derfor Internettstiftelsen i Sverige (IIS), som driver toppnivådomenet og registeret for alle .se-domener. IIS har informasjon som navn, adresser og telefonnummer til eiere av domener som slutter på «.se». I Norge har vi et tilsvarende selskap, kalt Norid.

Vi kontaktet IIS. Etter henvendelsen meldte de tilbake at det skulle være mulig for oss å få mer informasjon, siden det aktuelle domenet var privateid. Men de leverer ikke ut slik informasjon uten videre, og vi måtte derfor sende en skriftlig og begrunnet søknad, som skulle vurderes av jurist.

Et par uker senere ble søknaden innvilget og vi fikk kontaktinformasjonen til den som hadde registrert domenet Slettamig.se. Vi følte for første gang at vi var på sporet av noe: Vi fikk utlevert navnet på en mann.

Idet vi begynte å gå informasjonen nærmere etter i sømmene, viste det seg at den var delvis eller helt falsk. Navnet vi fikk av IIS tilhørte en person som var utvandret fra Norge for en årrekke siden, og som etter alt å dømme ikke hadde noe med saken å gjøre. Mobilnummeret vi fikk oppgitt var ikke lenger i bruk, og e-postadressen som var brukt i registreringen inneholdt ikke navn eller andre ledetråder. Etter over en måneds arbeid kom nok en bom. Så langt var det 10-0 til «Oscar».

Falsk informasjon blir redningen

Etter en lang og mislykket jakt på reell informasjon om «Oscar» og hans handlinger, skulle det vise seg at falsk informasjon skulle bli nøkkelen for oss. Vi begynte å søke på kontaktinformasjonen vi hadde fått fra IIS i flere offentlige register på nett, som Domaintools, DomainBigData og SecurityTrails. Registrene har enorme oversikter over domener og eiere.

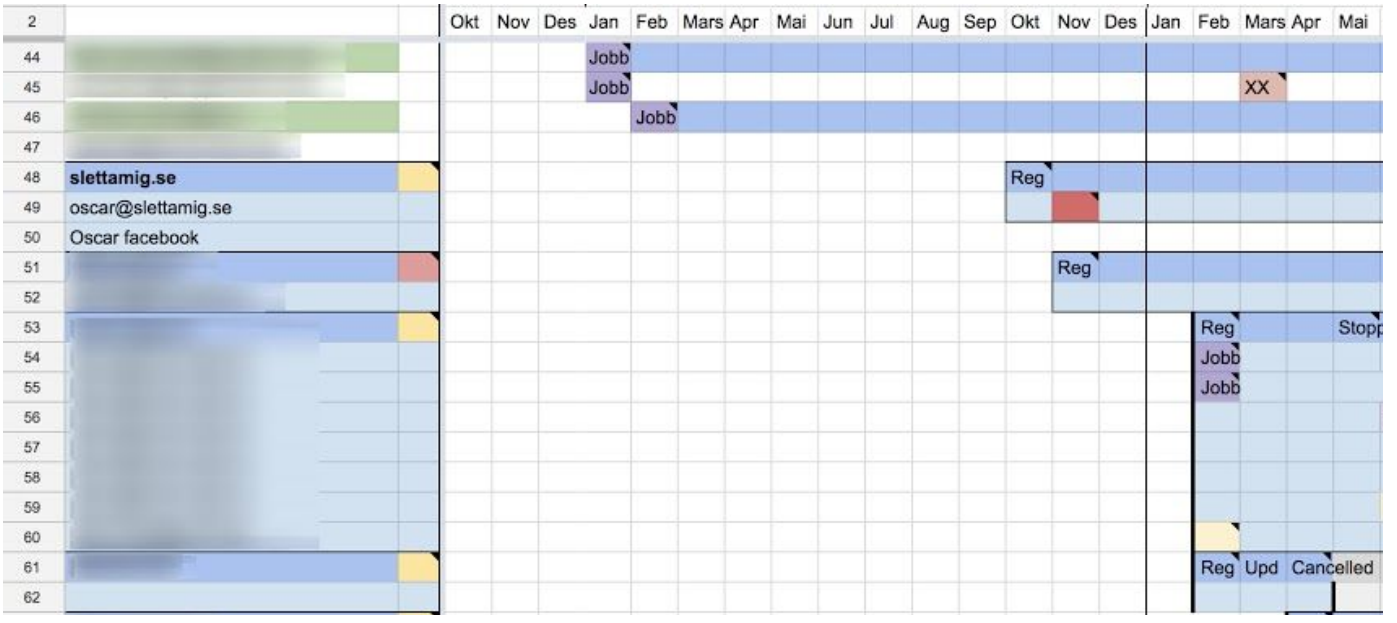
Søk på den falske kontaktinformasjonen ga treff. Vi oppdaget at flere domener, som inneholdt anerkjente merkevarer og navn, hadde blitt registrert på den samme falske kontaktinformasjonen. Vi gjorde også reverserte søk i SecurityTrails, noe som betyr at vi kunne søke opp andre domener som var opprettet eller tilknyttet den samme kontaktinformasjonen.

Her lærte vi noe nyttig: Falsk informasjon bør ikke alltid avskrives, men kan tvert imot være veldig viktig. Folk som ønsker å skjule seg, kan etter hvert miste kreativiteten og begynne å gjenbruke den samme falske informasjonen. De falske opplysningene vi hadde forbannet oss over tidligere, viste seg nå å bli selve nøkkelen til å komme videre i gravingen.

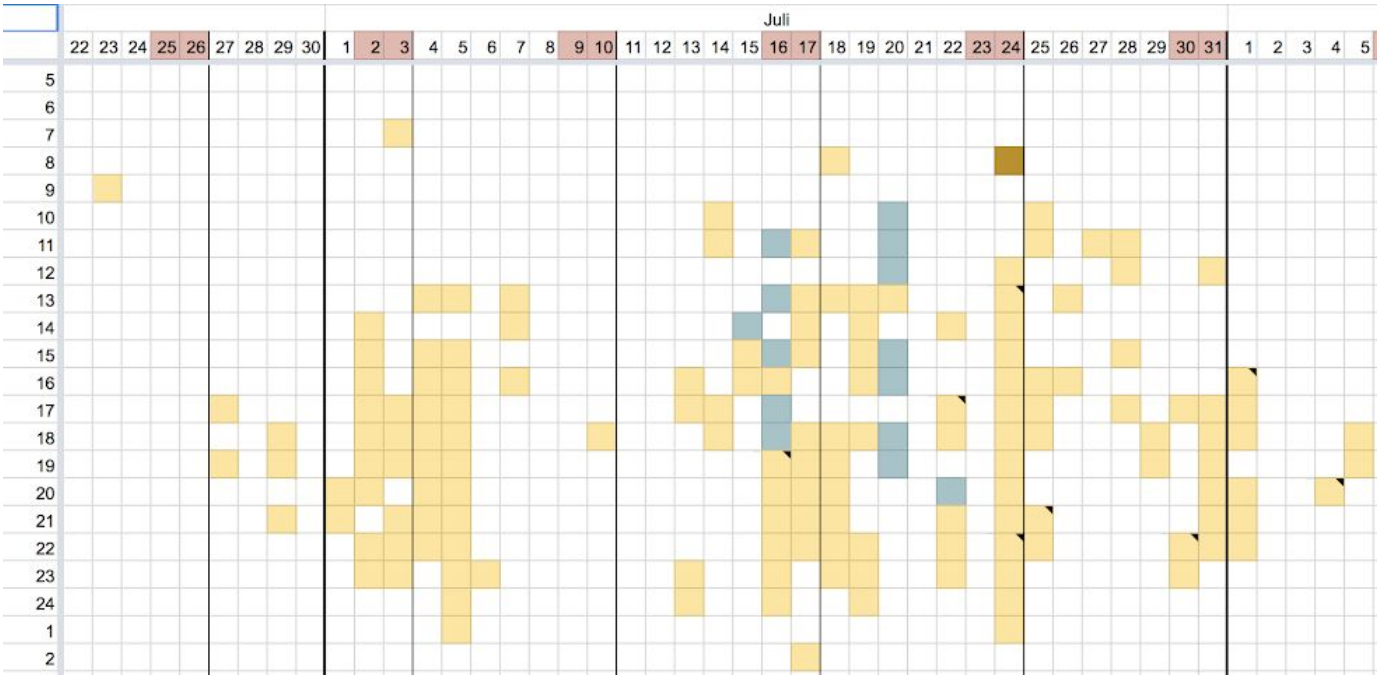
Systematisering, første runde

Etter hvert hadde vi fått mange ledetråder. Vi hadde kommunikasjon mellom Maiken og «Oscar», navn, adresser, telefonnumre, facebookprofiler, e-poster og en rekke nye domener. Vi måtte sikre at vi klarte å holde oversikten.

Vi opprettet derfor en ny tidslinje (et regneark). Her registrerte vi når domener hadde blitt opprettet og slettet (opplysninger som er synlige hos nettregistre som Domaintools, DomainBigData og SecurityTrails), når e-poster hadde blitt sendt, fra hvilke e-postadresser og når andre kontoer var aktive. Vi registrerte også nøye tidspunktene på døgnet «Oscar» kommuniserte med Maiken. Hver eneste melding og e-post ble plottet inn med tidspunkt, som kontaktpunkter mellom «Oscar» og Maiken. Vi brukte et regneark for å lage denne oversikten, med tid langs den horisontale aksen, og identiteter som e-post og domene langs den vertikale aksen.



Regnearket vi opprettet gav oss en god oversikt over aktiviteten til «Oscar» på tvers av kontoer og domener. Vi fargekodet ulike typer hendelser, som blant annet dato og tidspunkt for samtaler. Dette gjorde oss i stand til å se hvorvidt det var mønster i når «Oscar» var aktiv. Sensitive opplysninger er sladdet.



Basert på regnearket (se utsnitt over) laget vi også en mer detaljert oversikt, som var inndelt på aktivitet pr time (y-aksen) gjennom noen måneder i 2016 (x-aksen). Hvert kvadrat i figuren ovenfor er en hendelse fra en av «Oscars» kontoer. Flere av disse datapunktene fikk vi etter hvert også av andre kilder som hadde hatt korrespondanse med mannen.

Vi måtte ta høyde for at noen av de nye ledetrådene ikke nødvendigvis hadde noe med «Oscar» å gjøre. Vi registrerte derfor også med hvor stor sikkerhet vi kunne knytte ledetråden direkte til «Oscar». Hver gang vi fant en ny ledetråd måtte vi nøye gå gjennom oversikten og vurdere hvor sikkert eller usikkert det var at hver ledetråd var knyttet til «Oscar». Vi ga hver ledetråd en sannsynlighetsgrad basert på hvilke andre sikre koblinger vi hadde til ledetråden, og oppdaterte denne dersom nye opplysninger kom til fra andre kilder. Systematiseringen av materialet ga oss en oversikt med domener og e-poster vi visste «Oscar» stod bak. Takket være denne oversikten kunne vi nå slå fast at «Oscar» hadde vært aktiv i flere år, og at han hadde vært svært systematisk.

Denne måten å organisere materialet på, skulle også senere gi oss et viktig gjennombrudd.

5.2 Fase 2 – Utvidet søk

På dette tidspunktet var vi klar over at den falske kontaktinformasjonen ikke var nytteløs, men noe som ledet oss til ny informasjon. *Var gjenbruken av falsk informasjon et mønster, og kunne kontaktinformasjonen ha blitt brukt enda flere steder?*

Vi gjorde flere begrensede nettsøk på Google. Vi satte kontaktinformasjonen vi hadde i anførselstegn (fiktivt eks. “ola.nordmann@norge.no”). Da fikk vi opp resultater med innhold som stemte eksakt overens med søkefrasen vår.

Til vår store overraskelse ga søkene flere treff - på gamle stillingsannonser. De fleste lå åpent tilgjengelig på Karrierestart.no, og det var egentlig ikke noe bemerkelsesverdig med annonsene ved første øyekast. Men da vi tok en nærmere titt, gjorde vi funn som skulle bli svært viktige i jakten på «Oscar».

Analyse av annonser

Nå byttet vi arbeidsmetode fra digitale verktøy til markeringstusj. Vi printet ut alle stillingsannonsene vi fant. Med gul tusj markerte vi ord, setninger, oppgitte adresser og e-poster i annonsene for å gjøre en sammenligning.

Teamet brukte dette prosjektrommet underveis. Her hadde vi mulighet til å jobbe skjermet og lage oversikter over materialet.

Slik la vi merke til at stillingsannonsene hadde et særegent språk og inneholdt enkelte litt gammelmodige norske ord, som “husholderske” og “vertinne”. Med inspirasjon fra tv-serien «The Unabomber» benyttet vi delsetninger og ord fra stillingsannonsene vi hadde funnet, til å søke opp enda flere annonser. Vi fant ut at stillingsteksten noen ganger hadde blitt gjenbrukt uten, eller med kun små endringer i andre annonser. Det kunne tyde på at samme person sto bak.

Vi fant også andre likheter mellom annonsene. Det ble ofte brukt vilkårlige postadresser og de inneholdt sjelden telefonnummer. En annen fellesnevner var at søknad utelukkende skulle sendes på e-post.

Hvis «Oscar» stod bak stillingsannonsene, var dette en metode han brukte for å komme i kontakt med kvinner? Etter hvert skulle svaret på dette vise seg å være ja.

Stillingene som var utlyst hadde en slags rød tråd. De var stort sett innenfor serviceyrker som bartender, reiseleder, personlig assistent og vert/vertinne til arrangementer. Det ble sjelden stilt krav til kvalifikasjoner, og opplæring kunne gis av arbeidsgiver.

Mange av annonsene var åpenbart falske. For eksempel søkte et lite firma med én ansatt etter 15 nye deltidsansatte. En rask telefon til firmaeier bekreftet at annonsen var en bløff, og ikke laget av ham. Den oppgitte e-postadressen som søknader skulle sendes til, gikk heller ikke til det aktuelle firmaet.

Vi hadde tidligere i kartleggingen av domener lagt merke til at «Oscar» ofte benyttet e-postadresser fra en utenlandsk e-postleverandør. Et begrenset Google-søk på annonser knyttet til nettsted og denne leverandøren (eks. site:karrierestart.no + @protonmail.com) gjorde at vi fant enda flere annonser med lignende innhold.

Siden vi søkte så bredt etter jobbannonser, tok vi selvsagt høyde for at mange av annonsene vi fant ikke hadde noe som helst med «Oscar» å gjøre. Annonsene måtte sees i sammenheng med domenene og de e-postene i oversikten vår som vi visste han brukte. Gjennom arbeidet hadde vi bygd opp et godt kildenettverk. Det ble avgjørende for å verifisere om «Oscar» stod bak. Av hensyn til kildevernet kan vi dessverre ikke beskrive metodene vi brukte i dette arbeidet. Etter å ha silt ut mange annonser uten klare koblinger, kunne vi slå fast at et titalls av annonsene vi hadde funnet, var ført i pennen av «Oscar». Vi var på sporet, men skulle snart få ny motbør.

Innsyns-nei fra NAV

Noen av stillingsannonsene vi fant hos Karrierestart var hentet fra stillingsdatabasen til NAV. Dette var informasjon vi fikk oppgitt da vi kontaktet Karrierestart. *Kunne det ligge mer informasjon i annonsene? Og kunne NAV ha andre annonser vi ikke hadde klart å finne?*

Vi ba om innsyn i alle NAVs jobbannonser fra 2009 frem til 2018, i håp om at det kunne gi oss flere annonser eller mer informasjon. Det ble avslag. NAV svarte at jobben var for omfattende til at de kunne avsette ressurser. De foreslo en mulig løsning som ikke gjenspeilte vår forespørsel eller ivaretok våre behov.

Vi ville ikke gi oss, og i en ny e-post til NAV viste vi til Offentleglova §9: «Alle kan krevje innsyn i ei samanstilling av opplysningar som er elektronisk lagra i databasane til organet dersom samanstillinga kan gjerast med enkle framgangsmåtar.»

Vi påpekte at en eksport fra et moderne databasesystem ikke er en komplisert prosess. Vi viste også til at vi hadde forhørt oss med flere personer med kompetanse på de ulike teknologiene som var i bruk hos NAV. De bekreftet at det vi ba om ikke var en omfattende jobb.

Samtidig påpekte vi overfor NAV at deres utviklere i en video publisert på nett, forteller om datasystemene de bruker i den aktuelle portalen. Slik fikk vi også et godt innblikk i teknologiene som ligger bak, noe som hjalp oss i formuleringen av det nye innsynskravet. Vi tilbød oss også å ta i mot dataene i det formatet som var minst ressurskrevende for NAV. Vi fikk innsyn.

Det fremgikk imidlertid av materialet vi fikk, at databasen var ufullstendig. Vi oppdaget at flere av annonsene som lå ute på nettet, ikke fantes i databasen NAV sendte oss. Dermed måtte vi rette enda en henvendelse til NAV. Det viste seg å skyldes en feil, og til slutt fikk vi hele materialet.

Materialet inneholdt 449.706 annonser, og det ville vært en tidkrevende jobb å gå gjennom disse manuelt. For å enkelt kunne søke gjennom annonsene lastet vi dem inn i søkemotoren Solr. Solr er en søkemotor som på mange måter ligner på Google. Den gjør det svært enkelt å finne informasjon på tvers av mange dokumenter. Solr kan også gi treff selv om ordet du søker etter ikke har blitt skrevet korrekt. Derfor er Solr et bra verktøy hvis man skal søke gjennom store mengder dokumenter hvor det kan finnes feilstavinger.

Vi testet også en banebrytende metode som heter «authorship attribution». Det handler om å lære opp en datamaskin til å forstå skrivestilen til et individuelt menneske. Denne metoden ble opprinnelig brukt for å finne ut om usignerte tekster kunne tilhøre William Shakespeare, og har angivelig en god treffrate på skjønnlitterære tekster. Vi matet algoritmen med flere tekster som vi visste at «Oscar» hadde skrevet, i håp om at algoritmen skulle avsløre flere annonser i den store NAV-databasen. Til syvende og sist var ikke dette en god teknikk for dette formålet. Stillingsannonser i sin form er ikke spesielt kreative eller unike, og vi fikk en mengde åpenbare feiltreff fra denne algoritmen.

Vi fikk derimot en ny og viktig opplysning gjennom innsynet hos NAV. «Oscar» hadde klart å gå under radaren for NAVs sikkerhetsrutiner og registrert flere falske annonser i deres stillingsportal. Dette ble beklaget av NAV i en av NRKs oppfølgingssaker, og de bedyret at det jobbes med å bedre sikkerheten i deres systemer for å unngå nettopp slike hendelser.

Kartlegging av kilder

Vi hadde mye ny informasjon, men hadde fortsatt ikke funnet mannen. Vi hadde likevel funnet såpass mye at vi kunne gå bredere ut i jakten på nye ledetråder og kilder. Vi lagde en oversikt over alle som kunne ha informasjon som var nyttig:

- Eiere av kontaktinformasjon som var oppgitt å ha registrert ulike falske domener
- E-postleverandører og teleoperatører i inn- og utland
- Selskaper og privatpersoner som var blitt misbrukt i jobbannonser og e-poster
- Annonseportaler som NAV, Finn.no og Karrierestart
- Politiet

Mange av kildene vi kontaktet på dette tidspunktet ønsket ikke å bidra eller hadde ingen informasjon. Enkelte måtte også følge streng personvernslovgivning som forhindret dem i å gi oss informasjon. Flere av de vi kontaktet så ut til å være tilfeldige privatpersoner eller firmaer som hadde blitt dratt inn i saken ved at deres kontaktinformasjon var misbrukt.

Etter mye kildearbeid, kom vi i kontakt med flere som hadde blitt lurt av mannen vi lette etter.

Mye stod på spill for ofrene. De hadde tidligere blitt lurt med falske identiteter. Det viste seg at flere av ofrene var vanskeligstilte småbarnsforeldre som hadde blitt lurt av falske annonser som «Oscar» hadde lagt ut på en hjelpeside, drevet av Unicef, for personer som slet økonomisk. I disse annonsene utga han seg for å være firmaer eller privatpersoner som ville gi penger til familier som ikke hadde råd til ferie. Noen hadde delt personlig informasjon med «Oscar» i tro om at han var en god hjelper. Da de oppdaget at de hadde blitt lurt, fryktet de at informasjonen skulle bli brukt mot dem.

Vi jobbet mye med å bygge tillit, ved å møte kildene personlig og gi mulighet for å kommunisere gjennom krypterte kanaler (som Signal, en app som muliggjør kryptert kommunikasjon). I denne fasen kom vi endelig i kontakt med en person som hadde snakket med «Oscar» på telefon. Flere kilder ga opplysninger om at personen de hadde vært i kontakt med var en mann, og ga en antagelse på hvor i landet han kom fra, blant annet basert på dialekten.

Etter en langvarig prosess med en rekke kilder, satt vi på en stor mengde kommunikasjon som involverte «Oscar». I dette materialet, som vi ikke kan referere detaljert fra på grunn av kildevern, framstod «Oscar» som manipulerende, og som en person som trakasserte og truet.

Kilder kunne bekrefte antagelsen om at «Oscar» aktivt hadde brukt annonser for å komme i kontakt med mulige ofre. Deler av materialet vi hadde, inneholdt dokumenter og bilder fra «Oscar». Dette ble sjekket for metadata på samme måte som tidligere, men alt vi gjennomsøkte var helt strippet for informasjon.

«Oscar» gjør en tabbe

Det er imidlertid vanskelig å bløffe på heltid. Vi studerte alle e-poster fra kilder som hadde vært i kontakt «Oscar» og oppdaget at han noen ganger hadde blandet sammen egne e-postkontoer. En e-post-samtale med en kilde kunne starte på en e-postadresse, og deretter fortsette på en annen. Noen ganger ble dette trolig gjort for at han skulle fremstå som flere personer, andre ganger så det ut til å være en glipp. Måten vi fant ut dette på, var at vi kunne se at emnelinje og samtaleinnhold i e-postene var identiske, men at de plutselig fortsatte på en helt annen e-postadresse. Hos enkelte e-postleverandører er det mulig å bytte ut avsender av en e-post. Man benytter da en «sender address». I praksis betyr dette at det for mottakeren ser det ut som om e-posten kommer fra en annen adresse en den du faktisk sender fra.

Fordi samtalene plutselig fortsatte fra en annen e-postadresse kunne det virke som om «Oscar» hadde brukt en «sender address» for å skjule adressen han egentlig sendte fra, men glemt å bytte ut avsenderen senere i e-posttråden. Dette viste at *samme person* stod bak e-poster fra *ulike e-postadresser*.

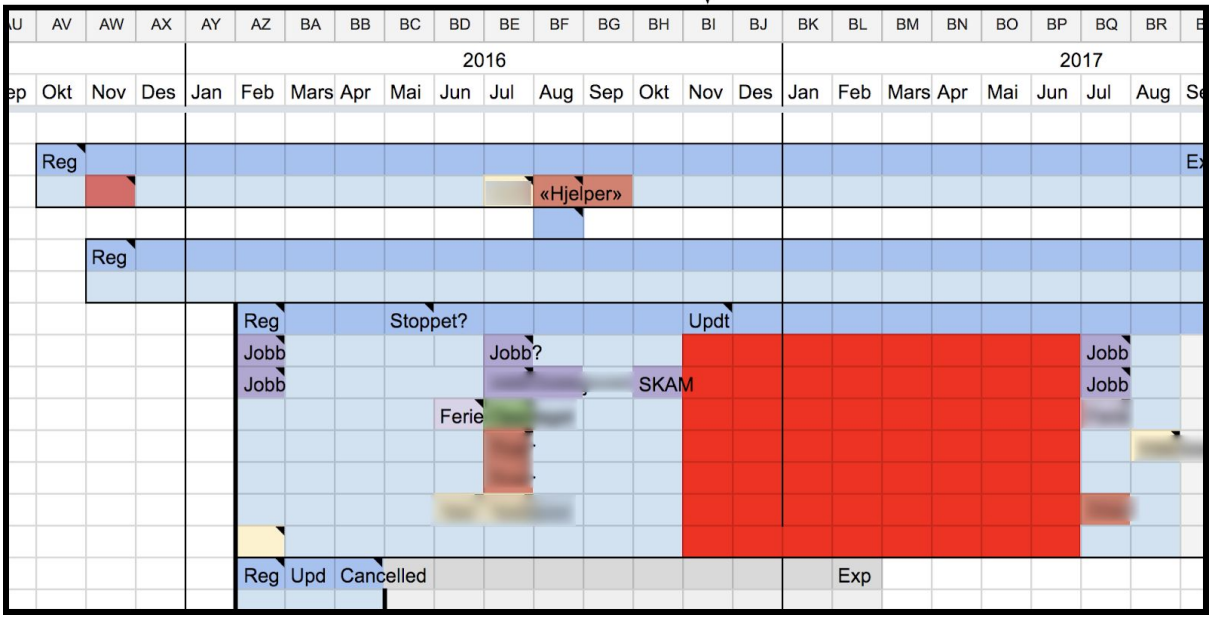
Og viktigst for oss; vi kjente igjen en av e-postadressene som plutselig dukket opp. Vi hadde kommet over den tidlig i prosjektet i forbindelse med en falsk jobbannonse fra 2012, men fant på daværende tidspunkt ingen tydelig tilknytning til «Oscar».

Nå visste vi at det var «Oscars» e-postadresse. Dermed ble den tidlige registreringen viktig for oss: Den viste at han hadde holdt på med falske annonser allerede for seks år siden. Funnet var en fin pay off for at vi hadde tatt vare på og lagt inn alle opplysninger i regnearket.

Partsinnsyn

På dette tidspunktet oppdaget vi noe som satte oss i en spesiell situasjon: Kildeinformasjon tilsa at også NRK hadde blitt misbrukt av «Oscar». Høsten 2016 ble en rekke norske unge kvinner på e-post forsøkt lurt til en falsk audition for NRK-serien Skam. Hendelsen ble omtalt i flere medier. NRK så alvorlig på saken, og hadde anmeldt misbruket til politiet, men saken var henlagt. Gjennom kildearbeid visste vi nå at «Oscar» var den som sto bak.

Etter at Skam-saken ble omtalt i media, så vi en drastisk endring i tidslinjen vår over «Oscars» aktivitet. Det oppstod et stort hull. Hullet, som er markert i rødt under, viser en total stopp i aktivitet fra «Oscar» i en lengre periode rett etter medieomtalen av Skam-svindelen.



Utsnitt fra tidslinje. Sensitive opplysninger er sladdet.

Det at bedriften NRK AS var en part i saken reiste noen problemstillinger. Ble vår rolle på noen måte endret av dette, og hvordan kunne det påvirke det journalistiske arbeidet med saken? Etter en runde med redaktører og juridisk avdeling i NRK, kom vi frem til at vårt redaksjonelle arbeid ikke burde eller skulle endre seg som følge av en sak NRK administrativt hadde vært involvert i. Det redaksjonelle arbeidet startet helt uten kunnskap om at NRKs bedriftsnavn hadde blitt misbrukt, og når det nå kom opp, var det rett og naturlig å behandle NRKs administrasjon som en kilde til informasjon – på lik linje med andre kilder.

Politiet startet etterforskning av saken, men den ble senere henlagt. Som part i saken ba vi om innsyn i etterforskningsmaterialet. Politiets metoder baserte seg i stor grad på grunnleggende bruk av Google og intervjuer med noen av de berørte partene. Vi så at vi hadde kartlagt mer enn politiet hadde gjort før saken ble henlagt, og at vi hadde sett sammenhengen mellom flere saker.

Takket være tidslinja oppdaget vi et nytt mønster i «Oscars» modus operandi. Han startet en utbredt praksis med å opprette domener der han framsto som firmaer. Med de nye domene framstod han trolig mer troverdig overfor nye ofre.

Feil mistenkt

Vi hadde nå en stor oversikt over e-poster og domener vi kunne knytte til «Oscar». Vi visste også hvor i landet han kom fra. Men fortsatt manglet vi hans faktiske identitet.

På dette tidspunktet, og med et bredere overblikk over «Oscars» virksomhet, kunne vi gå til kildene igjen med ny informasjon. Flere kilder vi kom i kontakt med ledet oss nå mot en konkret person. Dette fremsto som et stort gjennombrudd i saken. Endelig hadde vi ham. Trodde vi.

Vi begynte å gjøre intensiv research på vedkommende, gjennom offentlige registre, sosiale medier og tidligere medieomtale. Det var mange brikker som passet. Men da vi sjekket ham opp mot detaljer i vår egen tidslinje, kunne vi ikke overse at ting skurret. Vi måtte med kritisk blikk undersøke vårt eget materiale. Den aktuelle personen jobbet i utelivsbransjen, som medfører mye arbeid på kveldstid og natt. Dette sammenfalt svært dårlig med tidspunktene på døgnet vi i vår tidslinje hadde registrert at «Oscar» var aktiv. I tillegg stemte språkbruk i kildematerialet vårt dårlig med nasjonaliteten til personen som var blinket ut. Vi hadde feil person i kikkerten.

Ny taktikk

Vi begynte å tvile på om vi noen gang skulle klare å komme i mål. I prosessen til nå hadde vi ligget lavt for å unngå at den antatt meget datakyndige «Oscar» skulle merke at vi gravde i virksomheten hans. *Måtte vi nå justere taktikken for å ha sjangs til å finne ham?*

Var det noe viktig vi hadde oversett eller noen metoder vi ikke kjente til? Vi bestemte oss for å kjøre en form for kvalitetskontroll, og leide inn en ekstern IT-konsulent med høy kompetanse på digital sporing for å ettergå arbeidet vårt. Konsulenten, som ønsker å være anonym, gikk gjennom funnene våre så langt. Han kjørte også e-postadressene vi hadde samlet gjennom sine systemer i søken etter nye spor. Etter noen dagers arbeid konkluderte

vedkommende med at det gjenstod få andre alternativer enn å prøve omstridte og potensielt ulovlige metoder for å finne «Oscar». Å bruke ulovlige metoder var selvsagt ikke aktuelt. Konklusjonen var en viktig bekreftelse å få. Det var likevel nedslående, fordi vi ikke så mange flere muligheter i det videre arbeidet.

I stedet for å prøve å lure «Oscar» måtte vi gjøre noe vi lenge hadde kviet oss for å gjøre: Å åpent forsøke å opprette kontakt med ham. Vi kjente fortsatt ikke identiteten hans, og fryktet at en slik fremgangsmåte fikk ham til å gå under jorda, slette kompromitterende materiale og fortsette å plage Maiken og andre kvinner fra nye identiteter.

Vi valgte en mellomløsning. Vi kjente til en e-postadresse «Oscar» nylig hadde brukt til å utgi seg for å være en som jobbet med å fjerne nakenbilder på nettet. En i teamet sendte en e-post og presenterte seg som journalist i NRK. Han skrev at han jobbet med den samme problematikken og gjerne ville møtes. E-posten var utformet slik at «Oscar» ikke skulle skjønne at vi visste noe mer. Vi krysset fingrene.

Raskt kom en e-post i retur: Meldingen kunne ikke leveres til mottakeren fordi e-postadressen ikke lenger eksisterte. Vi hadde ingen andre e-postadresser å ta kontakt med «Oscar» på, uten å blåse at vi var på sporet av ham. Nå gjensto bare én mulighet. Vi måtte publisere; Vi hadde gjort mange funn i jakten på «Oscar». Ved å publisere funnene og Maikens historie, håpet vi å motta avgjørende tips.

5.3 Fase 3 – Publisering som metode

Vi oppsummerte det vi hadde dokumentert så langt:

- Maiken og flere norske kvinner hadde blitt utsatt for målrettet trakassering på nett av en ukjent mann.
- I over seks år hadde mannen drevet et kynisk maktspill gjennom et spindelvev av falske navn, e-postadresser og jobbannonser.
- Politiet hadde mottatt flere anmeldelser om mannen, men hadde ikke sett sammenhengen mellom flere saker hos ulike distrikt.

Vi måtte publisere saken med nok informasjon til at lesere gjennom tips kunne føre oss til «Oscars» ekte identitet. I artiklene ga vi mannen kallenavnet «Edderkoppen» - for å illustrere hans intrikate nett av falske identiteter.

Saken skulle ut i mange flater: På nett, på TV, i radio og i sosiale medier. Det var viktig å nå bredt ut for at aktuelle tipsere skulle få med seg saken. Vi opprettet en egen tipstelefon som gikk direkte til oss, og la inn tipsboks i sakene som viste hvordan vi kunne nås.

22. april publiserte vi saken om «Edderkoppen» og offeret hans Maiken. Vi publiserte også en kommentar om virksomheten hans, og sendte en reportasje i Søndagsrevyen.

Vi fikk umiddelbart stor respons.

Nøkkeltipset

De første timene etter publisering kom det inn mange telefoner og henvendelser. Allerede samme dag kom tipset som senere skulle gjøre det mulig for oss å avsløre «Edderkoppen».

En tipser fortalte oss om en episode for flere år siden. Tipseren hadde vært i kontakt med en person som kunne være «Oscar». Opplysninger denne tipseren ga samsvarte med flere av de sentrale opplysningene vi allerede hadde. Tipseren oppga blant annet en e-postadresse vi kunne kryssjekke mot informasjon i tidslinja vår.

Og aller viktigst: I deres digitale kontakt hadde «Oscar» begått en feil – han hadde sendt fra seg metadata hvor hans ekte navn lå begravd.

Personresearch

Vi hadde endelig et navn med sterke indisier på at dette var rett person. Med informasjon fra Folkeregisteret, skattelister, diverse nettsøk, tidligere medieomtale og kontoer i sosiale medier fikk vi dannet oss et bilde av personen. Vi hadde dokumentert at «Oscar» opptrådte hensynsløst og målrettet. *Kunne det hende at han var straffedømt?* Vi sjekket domsregistre i nærheten av der han bodde. Det ble blink.

En dom fra flere år tilbake viste at mannen hadde begått lignende handlinger tidligere. Dommen beskrev manipulative tendenser som minnet sterkt om de vi hadde sett i korrespondansen vi hadde lest.

Vi sjekket informasjonen i dommen opp mot informasjonen vi allerede hadde i tidslinja. Igjen skulle det vise seg at arbeidet med tidslinja gav uttelling: Vi sammenlignet adressene gjengitt i dommen med adressene vi hadde registrert i tidslinja. Flere av dem var identiske.

Vi var nå helt sikre: Vi hadde funnet «Oscar».

5.4 Fase 4 – Konfrontasjon

Vi hadde mannen, og visste hvor han bodde. Sammen med flere redaktører satte vi oss ned for å vurdere hvordan vi skulle få kontakt med mannen, og hvilke sikkerhetstiltak vi burde ta. Før vi i det hele tatt tok kontakt med mannen, bestemte vi oss for å forsøke å ordne et møte på våre premisser. Vi booket et møterom i byen hvor mannen oppholdt seg.

Vi kom fram til at det var lurt å sende flere journalister og en arbeidsleder, både av hensyn til sikkerhet og fordi det var en uoversiktlig situasjon: *Ville mannen prøve å stikke av? Kunne han bli voldelig?* Vi måtte vurdere alle muligheter. I lys av opplysningene fra dommen vi hadde funnet, kunne han reagere på mange ulike måter.

For en mann som har bedrevet såpass omfattende aktivitet på nettet, var det usedvanlig vanskelig å finne mannens telefonnummer. Gjennom kildearbeid fikk vi til slutt tak i nummeret. Da vi fikk kontakt med mannen valgte han ganske umiddelbart å legge kortene på bordet. Han gikk også med på å møte oss.

Planen om møterommet gikk skeis. «Oscar» ville ikke møte oss på et sted hvor han kunne risikere å møte bekjente. Det førte til at vi i stedet hentet «Oscar» i bil på et sted han foreslo, og fant et passende sted for intervjuet.

Mannen var tydelig nervøs og preget av situasjonen. Han var likevel åpen og villig til å fortelle i detalj, slik at vi også kunne ettergå opplysningene han kom med. Endelig hadde vi funnet «Oscar» og fikk hans detaljerte redegjørelse for metoder og motiv. Han var svært opptatt av at han i perioder ikke klarte å styre seg selv, og ga uttrykk for at han var veldig lei seg overfor sine ofre.

31. mai 2018, seks måneder etter at vi startet gravingen, publiserte NRK avsløringen på nett, TV og radio. Mannen bekreftet at han i flere år har plaget kvinner på nett, men hevdet overfor NRK at han ikke hadde noe med lekkasjen av Maiken-bildene å gjøre.

6. Konsekvenser

- NRK klarte å spore opp og avsløre mannen som stod bak trakasseringen av Maiken og et stort antall norske kvinner.

- Politiet hadde tidligere henlagt anmeldelser fra flere kvinner om mannen, blant annet fordi de ikke klarte å avdekke hans identitet. Etter NRKs saker iverksatte politiet ny etterforskning, koordinert over flere politidistrikt. Det endte med at mannen ble pågrepet. Han har tilstått i politiavhør, og er nå siktet for hensynsløs adferd.

- NRKs saker om «Edderkoppen» utløste stort engasjement og debatt om politiets arbeid med slike saker og det å bli et offer på nett.

7. Etikk

Anonymisering av «Oscar»

Vi identifiserte ikke «Oscar» i våre saker. Det lå en rekke vurderinger bak denne beslutningen, blant annet informasjon som kom frem i dommen som hadde falt flere år tilbake. Videre førte en totalvurdering av hans livssituasjon til at vi ikke fant det riktig å identifisere ham. Av samme årsak kan vi dessverre ikke gå inn på innholdet i vurderingene.

Kildevern og forholdet til politiet

Politi og media kan ofte ha sammenfallende interesser, men har ulike roller og oppgaver i samfunnet. Som journalister kunne vi ikke overlevere upublisert materiale til politiet, til tross for at det kunne ha samfunnsmessige gevinster og bidra til å oppklare en politisak. Vi kunne heller ikke gjøre dette fordi vi verner om våre kilder, og hadde garantert kildevern til flere. Utad og til ofre var dette til tider krevende å formidle, kanskje særlig fordi vi ikke navnga «Oscar».

Det var og er viktig for oss å opptre uavhengig av statsmaktene – at vår research og avsløring ikke ble en del av politiets etterforskning og at vi dermed kunne bli sett på som en «hjelper» for påtalemyndigheten.

8. Nyttige erfaringer

Finne eier av et kontonummer: På et tidspunkt i prosjektet hadde vi et kontonummer vi var nokså sikre på kunne lede oss direkte til «Oscar». Dette er ikke nevnt tidligere i rapporten, fordi det viste seg å være et blindspor. Banker er underlagt svært strenge krav til personvern og kan ikke uten videre utlevere navnet på hvem som eier en konto til utenforstående. Men hos enkelte banker vil navnet på den som eier en konto likevel dukke opp i en kontoutskrift dersom man overfører penger til kontonummeret. Dette testet vi reportere oss i mellom ved å overføre små summer til hverandre. I enkelte banker dukket navnet på mottaker opp i transaksjonsoversikten etter at overføringen var bokført.

Digital tidslinje: Å lage en tidslinje hvor vi la inn når aktiviteten fant sted (år, måned, dag, klokkeslett) gjorde også at vi etter hvert som vi fikk flere datapunkter inn i systemet, kunne se akkurat hvilke ukedager og når på døgnet den vi lette etter var aktiv. Det var verdifull informasjon når vi senere fikk utpekt personer. Her bidro tidslinjen direkte til at vi oppdaget manglende samsvar mellom aktiviteten i vår tidslinje og arbeidssituasjonen til den utpekte. Dette bidro til at vi fikk sjekket ut en uskyldig person av saken.