Undersökning av Tinder

Aron Ingemarrson, ar0667in-s@student.lu.se
Tilda Kylesten, ti3406ky-s@student.lu.se

***Abstract*— Den här rapporten undersöker den internetbaserade applikationen Tinder. Målet med undersökningen var att besvara två frågeställningar, vilka innefattade vilka protokoll som används samt om datatrafiken skiljer sig markant mellan vid användning av Tinders funktioner. Undersökningen utfördes framförallt med hjälp av programmet Wireshark. Tinders IP-adresser identifierades genom uteslutningsmetod och tre IP-adresser nyttjades vid funktionsanvändande. Dessa visade sig vid upprepning av försöken att de ej var statiska. Tinders olika funktioner testades vilka visade att det krävs aktivt användande för att trafik ska uppstå. Förutom att ladda upp bilder, som var mest datakrävanade, krävde swipe-funktionen något mer data än att skicka meddelanden. De identifierade protokollen var TCP samt TLSv1.2 vilket är ett säkerhetsprotokoll. Undersökningen hade kunnat förbättras genom bättre filtrering vid paketfångsten i Wireshark, men resultaten bedöms ändå som trovärdiga.**

I. Introduktion

I dagens samhälle används mobilen i allt större utsträckning och för varje dag som går uppkommer nya användningsområden. Nätdejting är ett fenomen som på senaste blivit allt mer populärt, enligt en SIFO-undersökning inleds var fjärde kärleksrelation på nätet. [1] Att marknadsföra sig själv på en dejtingsajt är utelämnande och det är viktigt att ens aktivitet i applikationen inte hamnar på villovägar. Denna rapport undersöker applikationen Tinder med fokus på vilka försiktighetsåtgärder som vidtagits för att skydda användarna, hur paketinnehållen varierar samt vilka protokoll som används beroende på applikationens funktion.

II. Bakgrund

Tinder är en dejting-applikation som bygger på att underlätta dejtandet genom att möjliggöra mötet med andra som du i vanliga fall troligen inte kommit i kontakt med. Applikationen är platsbaserad där det är möjligt att filtrera bort användare som befinner sig för, vad man själv anser, är för långt bort. På så sätt får man endast upp personer i sitt flöde som befinner sig i närheten. Huvudsyftet med applikationen är att användare endast ska ha möjlighet att kontakta varandra om båda parter visat intresse. Att visa intresse för en annan användare görs genom "swipe-funktionen", där en swipe åt höger på en profil visar intresse, medan en swipe åt vänster betyder att man inte är intresserad. Detta görs genom att dra fingret fram och tillbaka över skärmen. Om två användare har swipat höger på varandra matchas dem och blir tillgängliga för vidare kontakt, genom "chatt-funktionen".

III. Frågeställning

Syftet med rapporten är att undersöka hur paket och dess innehåll som skickas till och från Tinder varierar beroende på vilken funktion som används i applikationen, det vill säga om användaren swipar eller chattar. Vidare är det intressant att undersöka vilka protokoll som används samt om de ändras beroende på funktion. Konkret vill vi ta reda på:

- Vilka protokoll används vid respektive funktion? Är någon av dessa så kallade säkerhetsprotokoll?
- Kräver någon av funktionerna markant mer datatrafik i jämförelse med den andra?

IV. Metodbeskrivning

Applikationen Tinder undersöktes med hjälp av sniffer-programmet Wireshark. Tinder körs via webbläsaren Google Chrome och kräver därför anslutning till internet. Datorn som applikationen kördes på var uppkopplad till internet via Wifi till nätverket eduroam på Lunds Universitet. Anslutning hade en hastighet på 10 Mbit/sekund för både upp- och nedladdning.

Innan undersökningarna startades stängdes datorns internetapplikationer av samt flertalet bakgrundsprocesser avslutades för att minimera störningar från andra program. När detta var gjort startades först Wireshark, där fångst av paket initierades och data började analyseras. Sedermera startades webbläsaren Google Chrome och webbadressen tinder.com skrevs in och hämtades. För att ta reda på vilka IP-adresser som tillhörde Tinder genomfördes fyra tester, varav två bestod av att endast starta applikationen och låta den vara igång i 120 s och de andra två bestod av att starta igång applikationen och därefter använda funktionen swipe i 120 s. Efter varje genomfört test noterades alla IP-adresser som skickat data över 10 000 bytes.

Från dessa listor kunde vi sedan se vilka typer av IP-adresser som förekommer frekvent likväl vilka IP-adresser som mest data skickas ifrån. Detta gjordes för att kunna göra rimliga antaganden om vilken, eller vilka, IP-adresser som tillhör Tinder. När de troliga IP-adresserna väl hade identifierats fortsatte datainsamling genom fler tester. Dessa tester bestod i att först gilla sex stycken profiler på rad, respektive ogilla sex stycken profiler på rad. Vidare testades chatt-funktionen och vad som hände vid ändring av de personliga inställningarna.

När testerna var genomförda analyserades dessa i Wireshark för att extrahera tillgänglig data, samt bandbredden mättes med verktyget I/O-graphs.

V. Validitet & Begränsningar

En felkälla i studien är filtreringen av IP-adresser. Risk finns att relevanta IP-adresser filtrerats bort alternativt att irrelevanta adresser inte filtrerats bort, vilket kan leda till felslag i analysen av mängden datatrafik för Tinders olika funktioner. Emellertid är det inte av stor betydelse att datatrafiken blir helt korrekt; det viktiga är snarare att identifiera mönster och förstå hur applikationen fungerar i stora drag, för att sedan ha tillräckligt med underlag för att kunna svara på studiens frågeställning. Ytterligare en felkälla är avgränsningen av de olika testerna. Somliga har gjorts under ett bestämt tidsintervall, således är de jämförbara med varandra. Vissa av testerna har dock innefattat ett förutbestämt förlopp i applikationen, exempelvis att sex profiler ska gillas. Därefter har Wireshark stängts av. Det finns en risk för att de olika testerna har pågått olika länge, följaktligen är testerna inte helt jämförbara med varandra. Slutligen är en begränsning med studien att applikationen som undersöks endast nås via webbsidan, vilket försvårar analys av data då det inte går att undgå trafik kopplat till chromes webbläsare, exempelvis så kallade google-ads.

VI. Resultat & Diskussion

A. *Identifiering av IP-adresser*

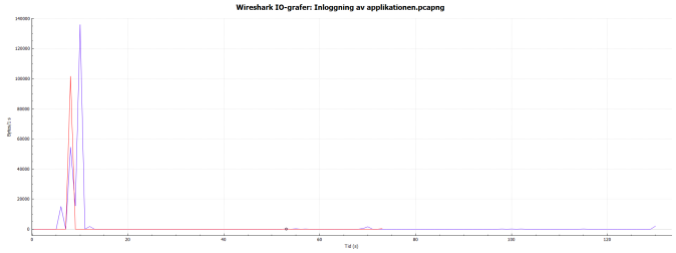
Omfånget på antal IP-adresser som fångades i Wireshark vid användning av Tinder var stort. Även om IP-adresserna inte var statiska noterade vi att många IP-adresser var liknande. Särskilt intressanta är de IP-adresser som förekommer ofta samt de vars datatrafik ökar när applikationen används, eftersom de med stor sannolikhet uppkommer vid användandet av Tinder. Adresserna som uppfyller något, eller båda dessa kriterier undersöktes vidare genom IP-adresserna ip2location.com som är en tjänst som bland annat rapporterar geografisk plats, domännamn och usage type. Resultatet presenteras i tabell 1.

Tabell 1. Exempel på relevanta IP-adresser

IP-adress	Domännamn	Geografisk plats	Usage type
157.240.194.27	facebook.com	Stockholm, SE	Search Engine Spider
108.177.127.157	google.com	Mountain View, US	Data Center/Web Hosting/Transit
143.204.247.8	amazon.com	Köpenhamn, DK	Data Center/Web Hosting/Transit

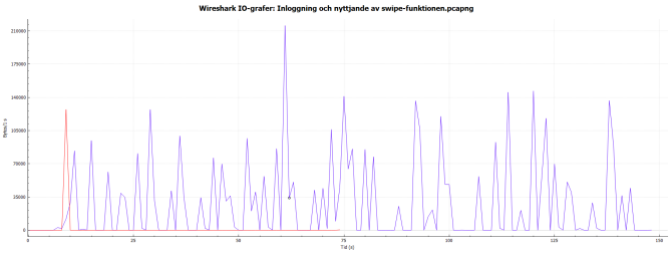
B. *Undersökning av olika funktioner*

Nedan följer resultat och diskussion för ett antal tester där vi varierade applikationens funktioner.



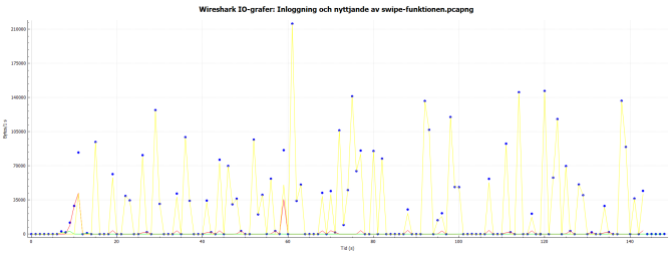
Figur 1. Inloggning av applikationen. Blå linje: 143.204.247.0/24 Röd linje: 157.240.194.27

Vid det första testet när Tinder kördes syns i figur 1 en tydlig ökning av datamängden i början, men när applikationen fick fortgå utan att några funktioner nyttjades syns en tydlig minskning i trafik. Det är också tydligt att IP-adressen tillhörande Facebook ökar sin dataöverföring strax innan Tinder loggas in vilket förmodligen beror på att Tinder använder Facebook som autentiseringsfunktion. Inloggning kan ske på annat sett, men det undersöks inte i rapporten. Vid inloggning gav Tinder upphov till en dataöverföring på 135 000 bytes/sekund medan Facebook nyttjar 100 000 bytes/sekund. Testet upprepades för att verifiera resultatet ytterligare och det gav liknande resultat.



Figur 2. Inloggning och nyttjande av swipe-funktionen. Blå linje: 143.204.247.0/24 Röd linje: 157.240.194.27

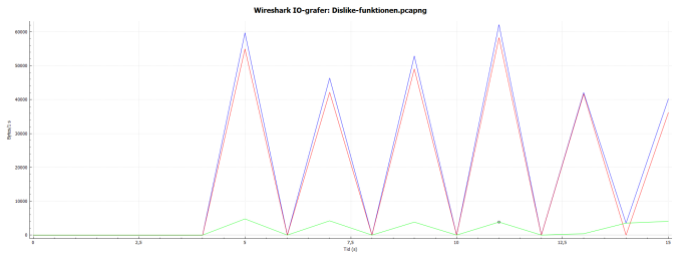
När applikationen testades genom, utöver att logga in, att även nyttja funktionerna “Like” och “Dislike” ökade mängden trafik markant. Swiparna och inladdning av profilerna representeras av de höga topparna i figur 2. Tydligt blir här också att inloggning med hjälp av Facebook enbart påverkar trafiken initialt, se den röda toppen i figur X. Den högsta toppen i detta test har en överföringshastighet på ca 210 000 bytes/sekund, men de flesta topparna ligger mellan 70 000-140 000 bytes/sekund. Anledningen till de varierande topparna beror förmodligen på att de olika profilerna innehåller olika mycket information. Återigen syntes liknande resultat när testet upprepades.



Figur 3. Trafikfördelning mellan IP-adresserna i filtret 143.204.247.0/24. Gul linje: 143.204.247.8 Grön linje: 143.204.247.101 Röd linje: 143.204.247.50, Blå punkter: 143.204.247.0/24

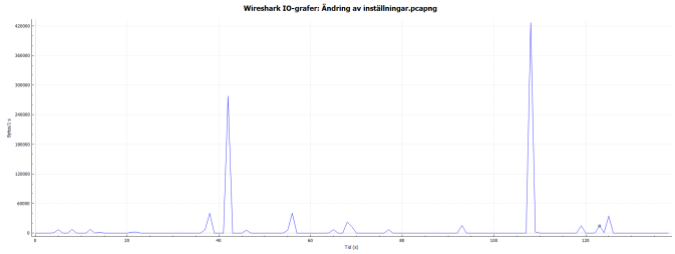
I figur 3 syns fördelningen av data mellan de olika IP-adresserna som ingår i filtret ip.addr==143.204.247.0/24 för testet som illustreras i figur 3. Det blir här tydligt att en IP-adress står för merparten av datan som skickas (gul linje), medan den andra IP-adressens (röda linjen) aktivitet är begränsad. Den är enbart aktiv vid inloggning samt ytterligare en gång, vilket skulle kunna bero på att den verifierar användaren med en förutbestämd frekvens. Den sista IP-adressen (grön linje) är till största del inaktiv. I och med att

datan regelbundet hämtas från en IP-adresser som liknar varandra är det också rimligt att anta att den hämtas från flera centrala servrar. Detta ter sig rimligt då informationen som skickas är väldigt privat och säkerhetsarbetet skulle försvåras om varje användare agerade som en server. Datamängden som skickas fram och tillbaka är också relativt liten vilket gör att de centrala servrarna klarar av belastningen.



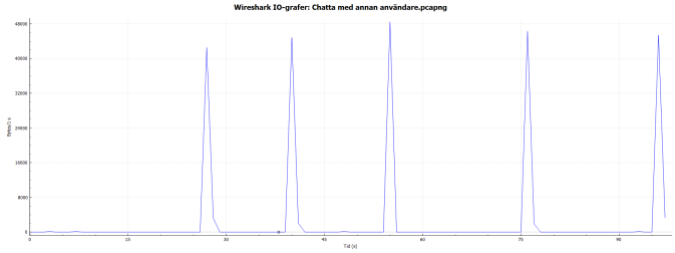
Figur 4. Dislike-funktionen. Blå linje: 143.204.247.0/24 Röd linje: 143.204.247.8 Grön linje: 143.204.247.128

I figur 4 har funktionen "Dislike" undersökts, speciellt hur olika IP-adresser samverkar vid användandet av funktionen. Vidare har dataöverföringen för två specifika IP-adresser som tillhör Tinder jämförts med den totala dataöverföringen som alla Tinders IP-adresser ger upphov till. De spetsiga topparna representerar varje gång använändaren tryckt på "Dislike". I figur 4 är det tydligt att flera IP-adresser samverkar vid användandet av en funktion, då både den gröna och den röda linjen bidrar till den blå linjen, det vill säga till att en "Dislike" sker. Vidare kunde konstateras att den maximala dataöverföringshastigheten under testet uppgick till 60 000 bytes/sekund. När testet modifierades något, mer specifikt att funktionen "Like" användes istället för funktionen "Dislike" resulterade det i en liknande graf.



Figur 5. Ändring av inställningar. Blå linje: 143.204.247.0/24

I figur 5 ses dataöverföringen av Tinder i samband med förändring av de personliga inställningarna. Som grafen visar är aktiviteten låg i princip hela tiden, förutom när vissa specifika inställningar ändras och sparas. Vid den högsta toppen laddades en ny bild till användarens profil upp vilket ledde till en momentan dataöverföring av 420 000 bytes/sekund.



Figur 6. Chatta med annan användare. Blå linje: 143.204.247.0/24

När användaren endast använder skrivfunktionen i Tinder blev det återigen tydligt att det bara är vid sändning av meddelanden som aktivitet sker, de olika topparna i figur 6 representerar sända meddelanden. Det största meddelandet använde 48 000 bytes/sekund.

Sammantaget för alla grafer gäller att applikationen i princip enbart skickar data när specifika funktioner används vilket gör det svårt att mäta någon genomsnittlig dataanvändning. Det är därför mer intressant att studera den momentana dataanvändningen vid de olika funktionerna och se hur de förhåller sig till varandra. Först när användaren använder en specifik funktion krävs någon större mängd dataöverföring, annars är aktiviteten i övrigt väldigt låg. De funktioner som kräver mest bandbredd är när olika profiler studeras och antingen gillas eller väljs bort. Detta beror förmodligen på att det kräver inladdning av nya bilder när profiler granskas. Ett undantag från detta uppmärksammas när en ny bild laddades upp till profilen, vilket krävde en större mängd dataöverföring än någon annan funktion.

C. Allmän analys

Det går inte med säkerhet säga om Tinder använder ett *Content Delivery Network* (CDN). Det är troligt att all trafik från Tinder inte går genom datacentret i Köpenhamn, emellertid har inget av de tester vi gjort bekräftat det. Likväl är en CDN en möjlig usage type för ip2location.com, vilket tyder på att Tinder inte använder CDN eftersom IP-adresserna kopplat till Tinder fick *Data Center/Web Hosting/Transit* som sin usage type.

Adresser som har facebook som domän har *Search Engine Spider* som usage type, även känt som *Web Crawler*. Det är en slags sökrobot som hämtar innehåll från olika webbsidor för att effektivisera sökfunktionen. [2] Eftersom vi inte hade facebook igång under testerna, men trafiken till dessa servrar ökade vid inloggning i applikationen antas att dessa servrar är delaktiga i autentingseringsstadiet av inloggningsprocessen.

De protokoll som användes när applikationen startades samt vid användning av applikationen var TCP och TLSv1.2. TCP är ett transportkontroll och TLSv1.2 är ett kryptografiskt säkerhetsprotokoll ovanpå TCP som ämnar skapa privat och säker kommunikation över internet. Transport Layer Security (TLS) består av tre komponenter: kryptering, autentisering och integritet. Kryptering innebär att datan döljs för utomstående parter, autentisering säkerställer att parterna som utbyter data är dem de utger sig för att vara och integritet-komponenten kontrollerar att datan inte har förfalskats eller ändrats. [3] Det är rimligt att TCP är det protokoll som huvudsakligen används, eftersom det anses vara väldigt pålitligt. På grund av noggrannheten i dataöverföringen är hastigheten lägre än exempelvis transportprotokollet UDP. [4] Tinder har inte lika stora krav på dataöverföringens hastighet som exempelvis onlinespel som använder transportprotokollet UDP, således är TCP att föredra.

VII. Sammanfattning

Då applikationen kördes genom en webbläsare uppstod problem med att identifiera exakta IP-adresser för Tinder. Den uteslutningsmetod som nyttjades kan därmed ej betraktas som felfri. Webbläsaren Google Chrome har många störningskällor,

bland annat i form av Google-ads. Det protokoll som används är TCP samt ett säkerhetsprotokoll som läggs ovanpå detta, vilket är TLSv1.2. Protokollen användes till alla de testade funktionerna i Tinder. Applikationen krävde ingen datatrafik så länge användandet var inaktivt, men så fort en funktion nyttjades ökade trafiken. De funktioner som kräver mest datatrafik är när nya bilder laddas in eller laddas upp, vilket är rimligt.

Referenser

[1] Carling, M., "Var fjärde relation börjar på nätet". SVD. Hämtad 12/12-19. https://www.svd.se/var-fjarde-relation-borjar-pa-natet

[2] Wikipedia, "WebCrawler". Hämtad 8/12-19. https://en.wikipedia.org/wiki/WebCrawler

[3] Cloudflare, "What is Transport Layer Security (TLS)?". Hämtad 4/12-19. https://www.cloudflare.com/learning/ssl/transport-layer-security-tls/

[4] Jinting, L., Lin C., Yuxiang, Z., Quanlong, G., "Extensive evaluation on the performance and the behavior of TCP congestion control protocols under varied network scenarios". Hämtad 23/12-19. https://www.sciencedirect.com/science/article/pii/S1389128618311265