3G-MOBIILILAITTEIDEN TCP/IP-LIIKENTEEN ANALYSOINTI

Jukka Laitila

Opinnäytetyö
Elokuu 2015
Tietotekniikka
Tietoliikennetekniikka ja
Tietoverkot

TAMPEREEN AMMATTIKORKEAKOULU
Tampere University of Applied Sciences

TIIVISTELMÄ

Tampereen ammattikorkeakoulu
Tietotekniikka
Tietoliikennetekniikka ja Tietoverkot

JUKKA LAITILA
3G-Mobiililaitteiden TCP/IP-liikenteen analysointi

Opinnäytetyö 54 sivua, joista liitteitä 18 sivua
Elokuu 2015

Nykyään hyvin suuri osa mobiiliverkkoihin yhdistyvistä laitteista on ns. älypuhelimia tai tablet-laitteita, jotka voidaan tässä yhteydessä niputtaa ns. älylaitteiksi. Kyseiset älylaitteet ovat erittäin suorituskykyisiä laitteita kaikin puolin. Niiden suuren lukumäärän sekä käyttöasteen takia mainostajat, laitevalmistajat sekä muut vastaavat tahot ovat todella kiinnostuneita keräämään tietoja kyseisten laitteiden käyttäjistä sekä heidän kiinnostuksen kohteistaan. Myös eri valtioiden viranomaiset ovat innokkaita keräämään tietoja älylaitteiden käyttäjistä kansallisen turvallisuuden nimissä, rikosten selvittämisessä tai poliittisin motiivein. Kaupallisilla tahoilla tietojen keräämisen motiivina voi olla esimerkiksi mainonnan kohdentaminen tai yleisesti mahdollisimman kattavien tietojen kerääminen, jotka edelleen voidaan myydä eteenpäin. Joskus tämä kaikki tiedon keruu tapahtuu käyttäjän tietämättä ns. ”konepellin alla”. Jotkin laitevalmistajat saattavat sisällyttää laitteen käyttöjärjestelmään tai esiasennettuihin sovelluksiin tietojen keruuseen tarkoitettuja osioita. Joissakin tapauksissa varsinkin ilmaisten sovellusten on todettu keräävän tarpeettoman paljon dataa ja lähettävän sitä eteenpäin useille palvelimille eri puolille maailmaa.

Tässä työssä tutkittiin joidenkin eri valmistajien 3G-verkkoa käyttävien älylaitteiden tietoliikennettä. 3G-laitteiden sen vuoksi, että vastaavia 4G-mittalaitteita tai älylaitteita ei ollut saatavilla. Työstä ei vallitsevissa puitteissa ollut mahdollista saada absoluuttisen aukotonta tai tyhjentävää. Pääasiallinen tarkoitus oli tutustua verkkoliikenteen analysointiin sekä käytettävään protokollapinoon. Painopiste oli ns. internetiin reitittyvän tietoliikenteen analysoinnissa.

Lähtökohtaisesti tutkittiin älylaitteen tietoliikennettä silloin, kun laite oli kytkeytyneenä 3G-verkkoon tai WLAN-verkkoon ja kun sitä ei varsinaisesti käytetty mihinkään. Laitteisiin ei ladattu mitään erityisiä sovelluksia, vaan tutkittiin laitetta sen käyttöjärjestelmän sekä omien esiasennettujen sovellusten puitteissa.

Laitteiden havaittiin lähettävän jonkin verran epämääräistä dataa eri puolille maailmaa. Osa liikenteestä oli osa normaalia toimintaa, osa taas oli mitä ilmeisemmin ns. ei-haluttua.

Asiasanat: internet, tietoliikenne, tcp/ip, mobiili, älylaite, älypuhelin, tablet-laite

ABSTRACT

Tampere University of Applied Sciences
Degree Programme in ICT Engineering
Telecommunication and Networks

JUKKA LAITILA
Analyzing TCP/IP-Traffic of 3G-Mobile Devices

Bachelor's thesis 54 pages, appendices 18 pages
August 2015

Nowadays a large part of devices connecting to mobile networks are so called smartphones or tablets, which can be in this matter combined as smart devices. These smart devices are extremely well performing and powerful. Because they exist in such great numbers and they are used very widely, advertisers, device manufacturers and other such parties have become very interested about collecting data about users of these smart devices. Also authorities of different countries are eager to collect data about the smart device users in the name of national security, crime solving or with political motives. Commercial parties may have motives to collect data, such as advertisement focusing or just to collect as much data as possible which can be sold forward. Sometimes this all happens without the users knowledge and so called "under the hood". Some manufacturers may include some data gathering sections in the devices operating system or in the preinstalled applications. In some cases it has been noticed that especially some free-of-charge applications have gathered unneccessary amount of data and forwarded it around the world.

The purpose of this thesis was to investigate network traffic of some different manufacturers devices which are capable of using 3G-networks. 3G-devices instead of 4G-devices just because the lack of suitable measuring equipment and smart devices. In these circumstanses it was not possible to make this investigation absolutely flawless. The idea was to get familiar with network analyzing and with the protocol stack. The main focus was in analyzing the traffic which routes to the internet.

The starting point was to investigate the smart devices network traffic when the device is connected in a 3G- or WLAN-network and the device isn't actually used in anything. The intention was not to install any specific applications in the device, but to investigate the device in the framework of its operating system and its preinstalled applications.

There were some indications that these devices sent some amount of strange-looking traffic around the globe. Some of the traffic was possibly completely normal but some of it were more likely unwanted traffic.

Key words: internet, telecommunication, tcp/ip, mobile, smart device, smartphone, tablet-device

SISÄLLYS

LYHENTEET JA TERMIT

ARP	Address Resolution Protocol, osoitteenselvitysprotokolla Ethernet-verkossa
DHCP	Dynamic Host Configuration Protocol, IP-osoitteiden jakamiseen tarkoitettu protokolla
DNS	Domain Name System, domain-nimien selvittämiseen tarkoitettu protokolla
DUT	Device Under Test, tutkittava laite
HTTP	Hyper Text Transfer Protocol, www-tiedostojen siirtämiseen käytetty protokolla
ICMP	Internet Control Message Protocol, verkon vikailmoituksiin käytetty protokolla
IGMP	Internet Group Management Protocol, multicast-istuntojen hallinnointiin tarkoitettu protokolla
IP	Internet Protocol, internet protokolla
NTP	Network Time Protocol, aikakyselyihin tarkoitettu protokolla
OSI	Open Systems Interconnection, ajattelumalli verkon eri tasojen suhteesta toisiinsa
PSK	Pre Shared Key, annalta jaettu avain
SSDP	Simple Service Discovery Protocol, Plug & Play palveluihin liittyvä protokolla
SSL	Secure Socket Layer, yhteyden salaamiseen käytetty protokolla
TCP	Transmission Control Protocol, tiedonsiirtoprotokolla
TCP/IP	Protokollapino
TLS	Transport Layer Security, yhteyden salaamiseen käytetty protokolla
URI	Uniform Resource Identifier, merkkijono tai yksikäsitteinen nimi
USB	Universal Serial Bus, universaali sarjaväylä
USIM	Universal Subscriber Identifier Module, mikrosiru, jonka avulla kytkeydytään mobiiliverkkoon
W-CDMA	Wideband Code Division Multiple Access, laajakaistainen koodijakokanavointi

WNS	Wireless Network Simulator, protokolla-analysaattorin sisältämä ohjelmisto
WPA	Wi-Fi Protected Access, langattoman verkon suojaustekniikka

1 JOHDANTO

Tässä työssä käytettävään laitekokoonpanoon ajauduttiin olosuhteiden pakosta. Tutkittavasta asiasta saisi huomattavasti kattavamman analyysin aikaiseksi viimeisimpää teknologiaa sisältävillä uusimmilla mittalaitteilla sekä tutkittavilla laitteilla. Työssä pyritään selvittämään ei-halutun tietoliikenteen määrää sekä kohteita niin hyvin kun se on vallitsevissa olosuhteissa mahdollista.

Ei-haluttua tietoliikennettä on mahdollisesti nykyään niin paljon, että se voisi jopa jossakin olosuhteissa vaikuttaa laitteiden suorituskykyyn sekä tietoliikenneyhteyksien nopeuteen.

Oppilaitokselta löytyvä 3G-protokolla-analysaattori pystyy simuloimaan tukiasemaa ja sen toimintaa, joten sen lisäksi tarvitaan vain PC, johon kanavoida kaikki liikenne. PC:ltä voi tarvittavilla ohjelmistoilla analysoida liikenteen suhteellisen tarkasti ja laitekokoonpano on muutenkin melko yksinkertainen eikä laitteiden konfigurointikaan ole osoittautunut mahdottomaksi.

Kaapattua tietoliikennettä eli ns. dumppia tutkitaan kulloisenkin älylaitteen lähiverkon IP-osoitteen perusteella.

2 MITTAUSVÄLINEET

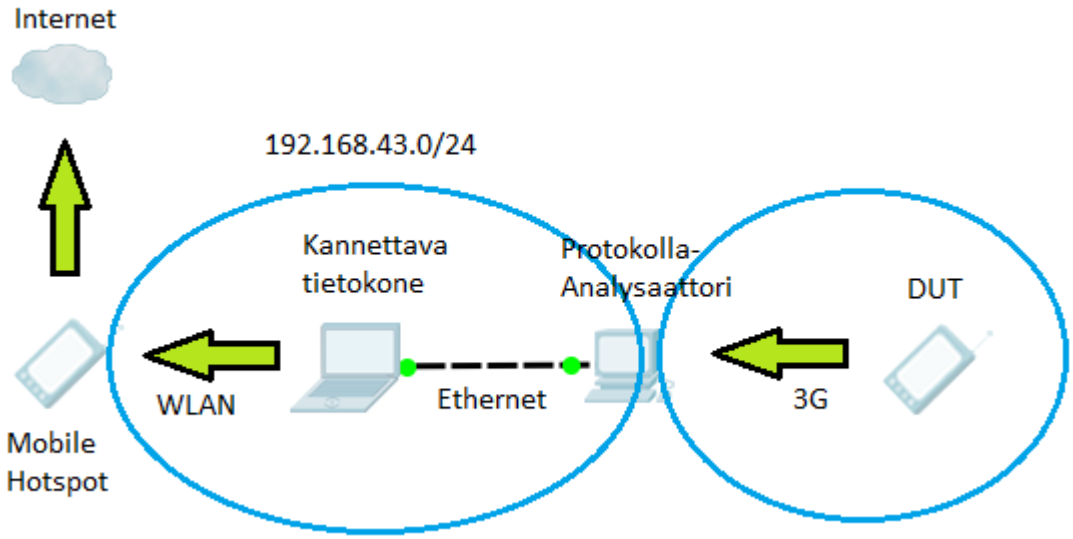
2.1 Laitteet sekä niiden asettelu

Työssä pyritään analysoimaan älylaitteiden aiheuttamaa internetiin reitittyvää tietoliikennettä sekä 3G-verkkoon, että WLAN-verkkoon kytkeytyneenä. 3G-verkkoon kytkeytymisen simulointiin käytettävä laite on Anritsu MD8470A –protokolla-analysaattori. Kyseinen laite simuloi 3G-tukiasemaa, johon testattava laite (DUT, Device Under Test) kytkeytyy. DUT:iin asetetaan Anritsun oma testi-USIM-kortti, jonka avulla yhteys saadaan muodostetuksi.

KUVA 1. Laitekokoonpano 3G-verkkoon kytkeytymistä varten

Kuvassa 1 vasemmassa alareunassa on testattava älylaite ja keskellä protokolla-analysaattori, johon on kytkettynä antenni radiorajapinnan muodostamiseksi sekä ns. lankapuhelimen luuri, jota tarvitaan, kun muodostetaan puhelu DUT:n sekä analysaattorin välille. Protokolla-analysaattori on käytettävyydeltään lähes kuin mikä tahansa normaali PC, ja siinä on käyttöjärjestelmänä Windows XP. Protokolla-analysaattori muodostaa DUT:n kanssa yhteyden radioteitse, ja yhteys ulkomaailmaan eli internetiin on muodostettu Ethernet-kaapelilla, jonka toinen pää on kytketty kannettavaan tietokoneeseen, jossa varsinainen tietoliikenteen analysointi tapahtuu. Järkevämpää olisi ollut analysoida data suoraan protokolla-analysaattorilla, mutta kyseisen laitteen vajavaisen toiminnallisuuden vuoksi tämä toteutettiin kannettavalla tietokoneella. Kannettava tieto-

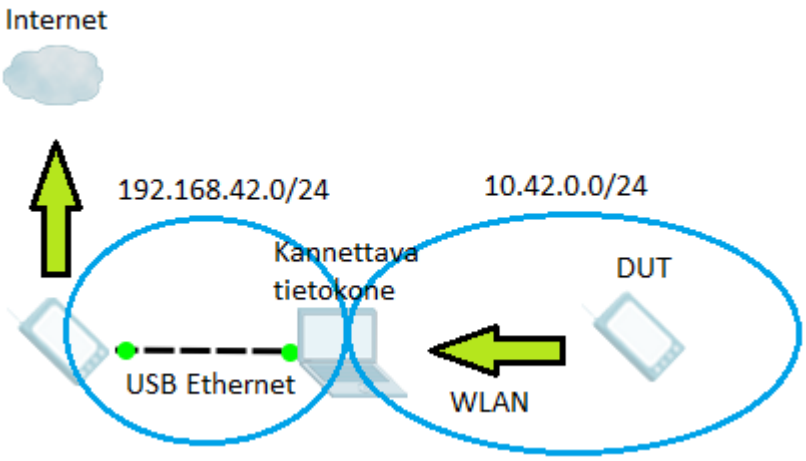
kone on yhteydessä WLAN-verkkoon, joka on muodostettu käyttämällä erään älypuhelimen Mobile Hotspot –toimintoa. Näin DUT on yhteydessä internetiin. Internetyhteyden muodostamiseksi olisi ollut monia muitakin vaihtoehtoja ja ratkaisuja, mutta tähän päädyttiin asetelman yksinkertaisuuden sekä käytettävissä olevien laitteiden saatavuuden vuoksi.



KUVA 2. Laitekokoonpano

DUT:n lähettämä kaikki internetiin reitittyvä tietoliikenne kanavoituu protokolla-analysaattorin sekä kannettavan tietokoneen välisen Ethernet-yhteyden kautta. Näin ollen kannettavan tietokoneen Ethernet–portin liikennettä analysoimalla voidaan seurata DUT:n internetliikennettä.

DUT:n liikennettä WLAN-verkkoon kytkeytyneenä voidaan tutkia niin, että kannettavasta tietokoneesta tehdään Wireless Access Point. Tässä tapauksessa käytetään kannettavan tietokoneen Linux Mint –käyttöjärjestelmän omaa Wireless Access Point –toimintoa.



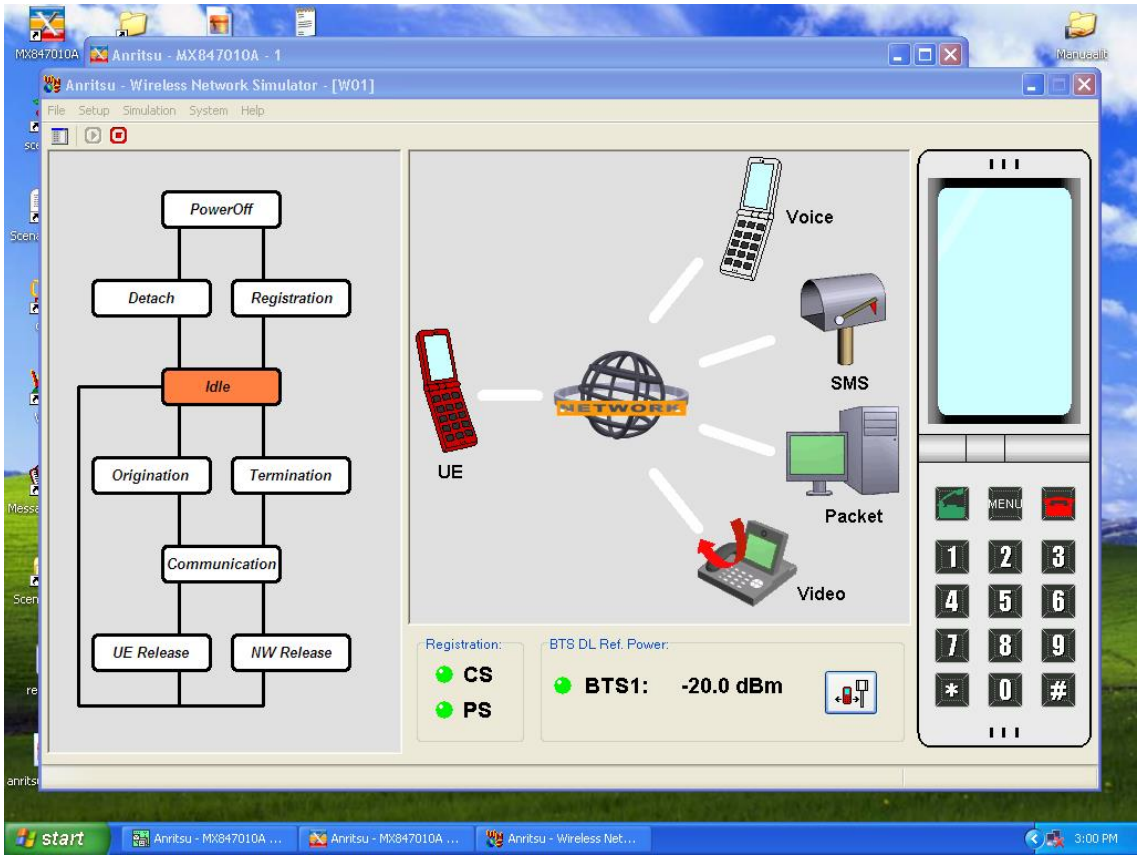
KUVA 3. Toinen laitekokoonpano

Kuvan 3 tilanteessa älypuhelin on mobiiliverkon kautta yhteydessä internetiin. Älypuhelin jakaa internet-yhteyttä kannettavalle tietokoneelle kaapelilla USB Ethernet -väylän avulla. Kannettavalla tietokoneella jaetaan samaa yhteyttä edelleen käyttämällä Wireless Access Point –toimintoa ja DUT kytkeytyy tähän jaettuun WPA-salattuun (Wi-Fi Protected Access) langattomaan lähiverkkoon PSK:n (Pre Shared Key) avulla ja näin ollen mikään muu laite ei voi käyttää samaa verkkoa. Wireshark-ohjelmalla voidaan tallentaa kaikki liikenne kannettavan tietokoneen WLAN-verkkokortilta. Kyseisessä WLAN-verkossa ei tapahdu käytännössä muuta kuin DUT:n liikennöintiä.

2.2 Käytettävät ohjelmistot

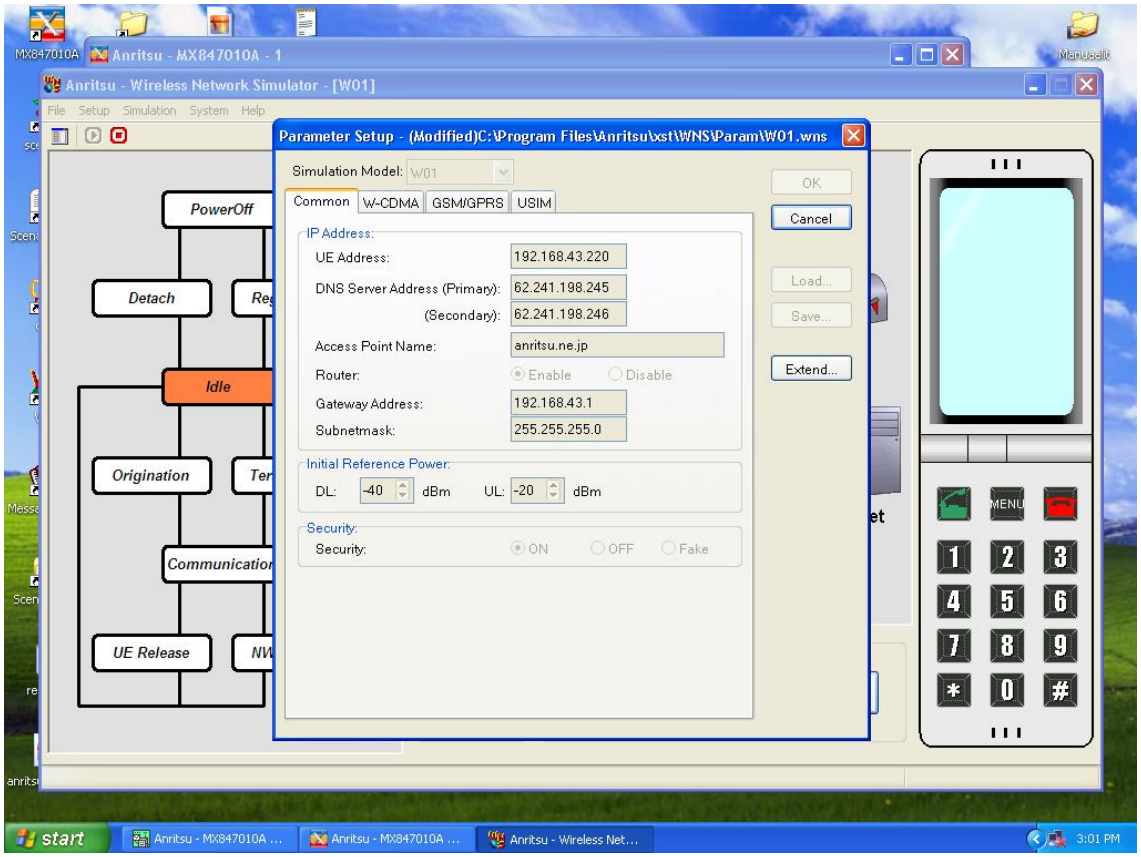
2.2.1 Wireless Network Simulator (WNS)

Tässä työssä tarvitaan Anritsu MD8470 –protokolla-anlysaattorin monista toiminnoista vain hyvin pientä osaa. 3G–yhdeyden simulointiin käytettävä ohjelmisto on WNS (Wireless Network Simulator), jonka avulla radiorajapinta saadaan muodostettua.



KUVA 4. Wireless Network Simulator –ohjelman perusnäkymä

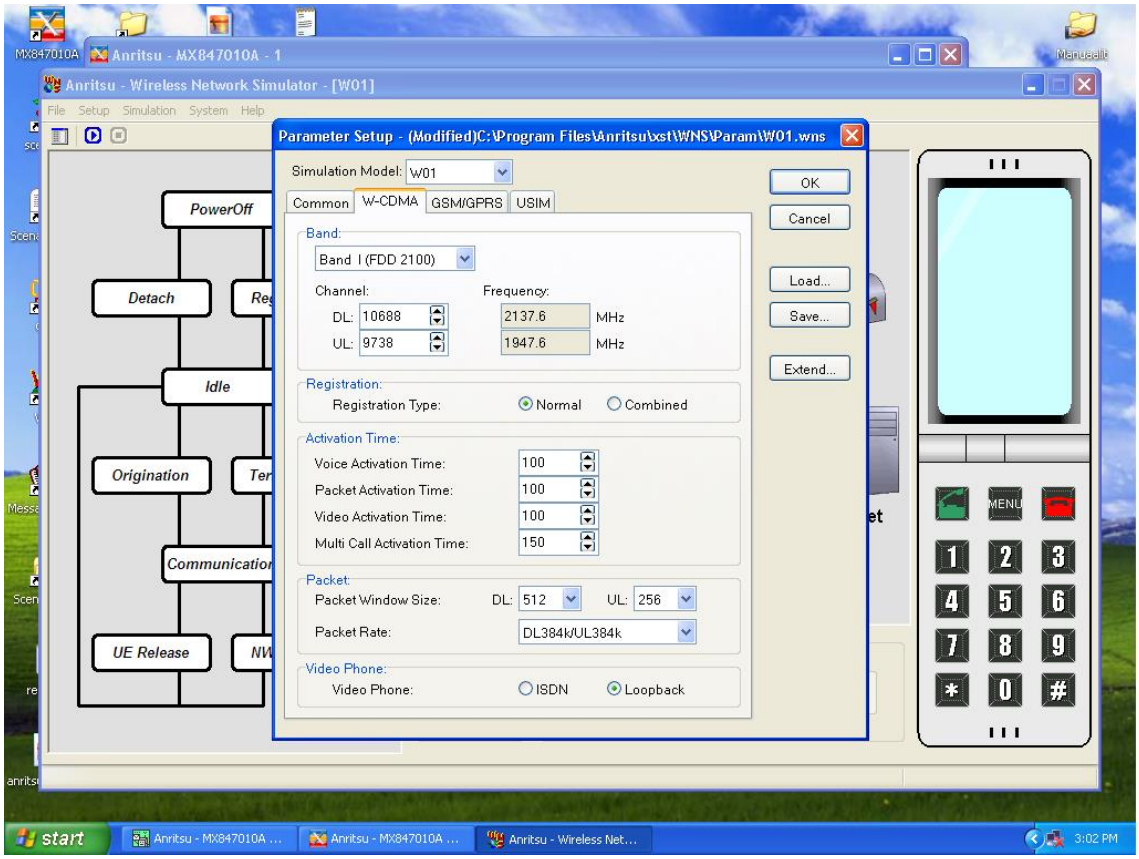
WNS:n perusnäkymä on hyvin yksinkertainen. Kuvan 4 tilanteessa DUT on kytkeytynyt simuloituun tukiasemaan ja on asettunut ns. Idle-tilaan. Kuvan 4 keskellä alhaalla BTS1-kohdasta voidaan säätää simuloidun tukiaseman lähetystehoa, jonka sai suurimmillaan -20 dBm:n tasoon, joka kaikki onkin tarpeen, jotta protokolla-analysaattorin käyttämä pieni antenni saa ylläpidettyä riittävän voimakasta signaalin tasoa. Kuvan 4 yläreunan Setup-kohdasta voidaan asettaa Parameter Setup -asetuksia.



KUVA 5. WNS:n Parameter Setup -näkymä

Kuvan 5 Parameter Setup -näkymässä asetetaan internetiin reitittymistä varten tarvittavia parametreja.

”**UE Address**” –kohtaan (User Equipment) asetetaan IP-osoite, joka annetaan DUT:lle. ”**DNS Server Address**” -kohtaan (Domain Name System) asetetaan tarvittavien DNS-palvelimien osoitteet, jotka ovat tässä tapauksessa DNA-verkko-operaattorin DNS-palvelimien osoitteet. ”**Access Point Name**” -kohtaan asetetaan nimi, jonka nimisenä DUT tunnistaa Access Pointin ja johon DUT:lla kytkeydytään. ”**Router**” –kohtaan asetetaan Enable, jotta internetiin reitittyminen olisi mahdollista**.** ”**Gateway Address**” –kohtaan asetetaan IP-osoite, jonka kautta on pääsy muihin verkkoihin eli tässä tapauksessa internetiin. Kyseinen 192.168.43.1 –osoite on älypuhelimen, jolla on muodostettu langaton lähiverkko (WLAN) Mobile Hotspot –toiminnolla, lähiverkko-osoite. ”**Subnetmask**” –kohtaan asetetaan kyseisessä lähiverkossa käytettävä aliverkon peite, joka on tässä tapauksessa 255.255.255.0.

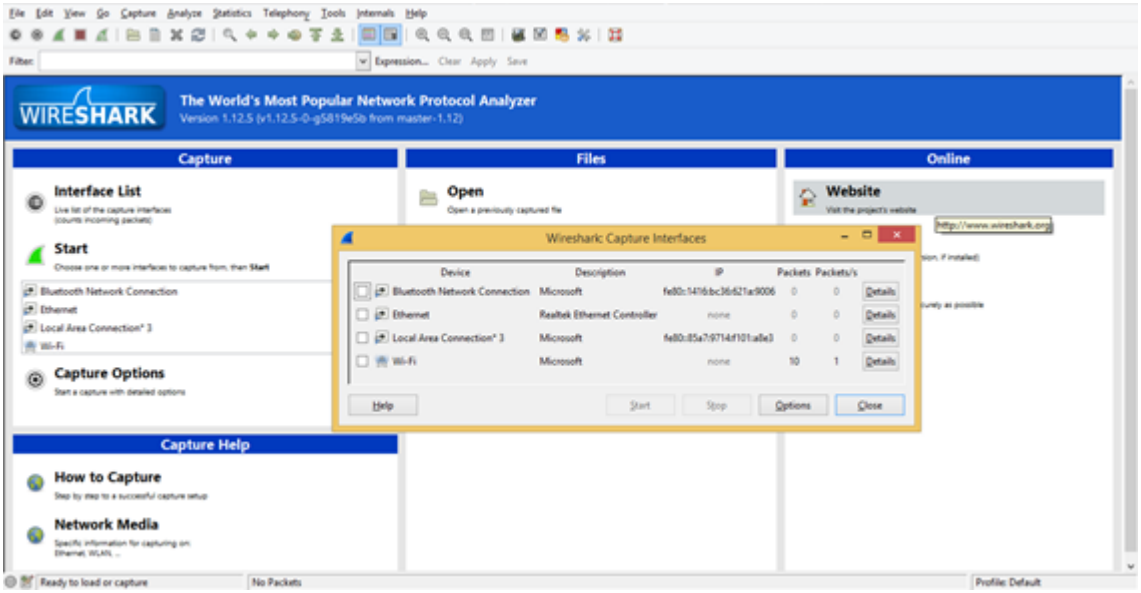


KUVA 6. WNS:n Parameter Setup W-CDMA välilehti

Kuvassa 6 olevat asetukset ovat ohjelmiston oletusasetuksia lukuun ottamatta Packet Rate -asetusta. Kyseisestä kohdasta voidan määrittää yhteyden nopeus ala- sekä ylävirtaan. Tuntemattomasta syystä ainoastaan kuvassa valittu ”**DL 384k/UL 384k**” –asetus osoittautui toimivaksi. Nykyaikana tämän tasoiset tiedonsiirtonopeudet eivät ole järin suuria ja käytettävillä laitteilla olisikin kapasiteettia ylläpitää huomattavasti suuremman nopeuden omaavaa yhteyttä.

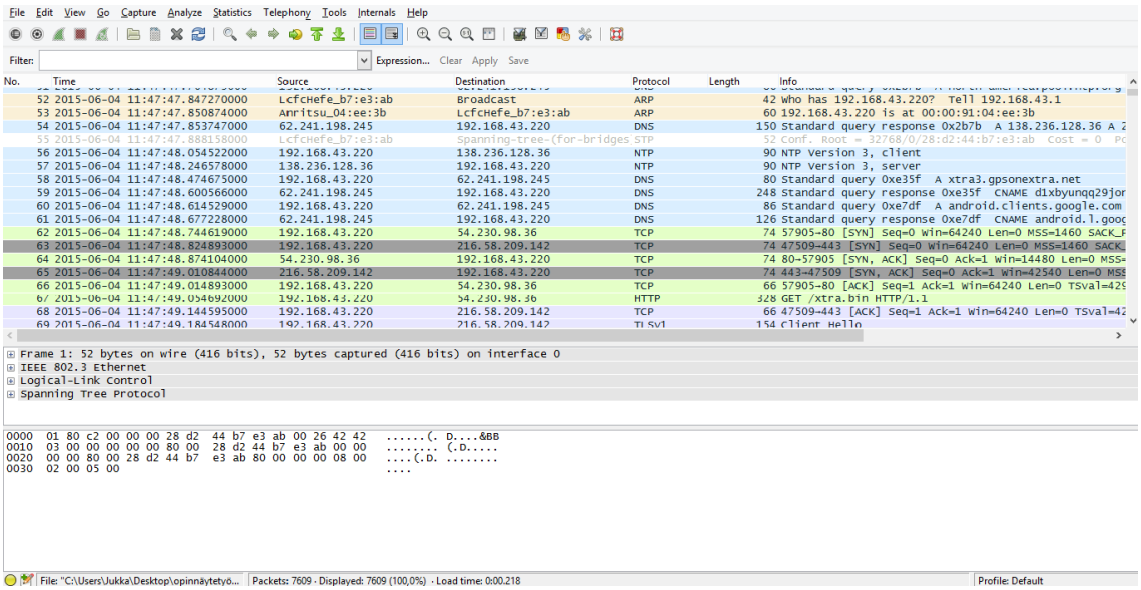
2.2.2 Wireshark

Varsinaista tietoliikenteen analysointia varten on kannettavalle tietokoneelle asennettu Wireshark–ohjelmisto. Wireshark on avoimeen lähdekoodiin perustuva työkalu datapakettien analysointiin. Sitä voidaan käyttää verkon vianhakuun tai verkkoliikenteen analysointiin. Yksinkertaisimmillaan valitaan vain verkkoliitäntä, minkä liikennettä halutaan kuunnella ja analysoida, ja käynnistää analysointi. Ohjelma tallentaa kaikkiin tuntemiinsa protokolliin perustuvan liikenteen, joka voidaan tallentaa .pcapng-tiedostoksi, josta voidaan jälkikäteen suodattaa eri osia analysointia varten.



KUVA 7. Wiresharkin perusnäkymä

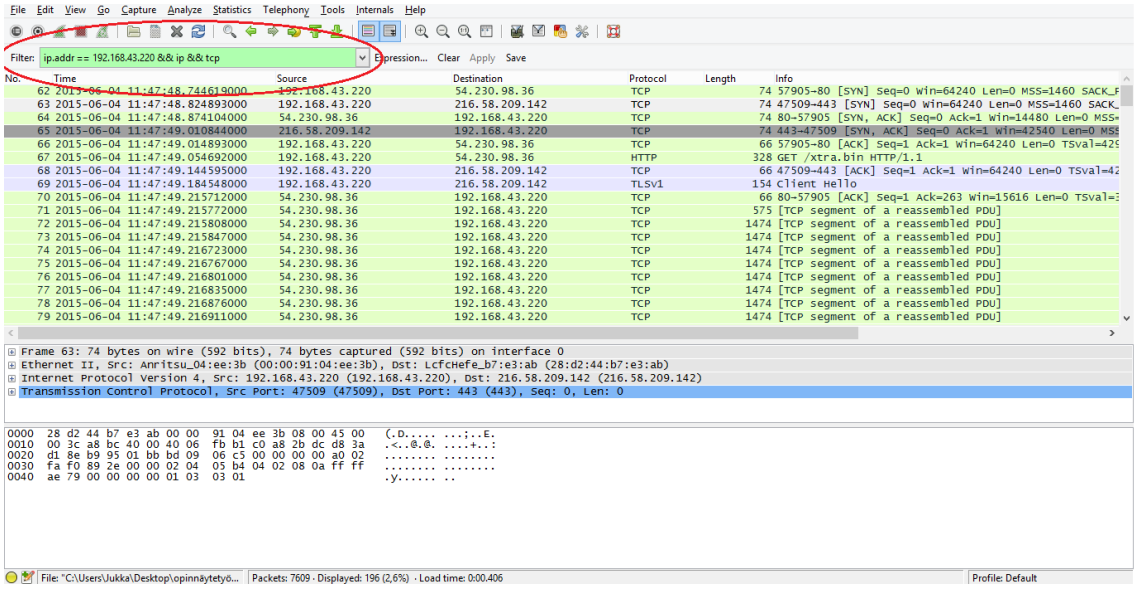
Kuvassa 7 on Wireshark-ohjelman perusnäkymä ja Interface List –kohdasta painettu ikkuna on avautuneena. Kyseisestä valikosta valitaan tässä tapauksessa Ethernet tai Wi-Fi, koska niitä liitäntöjä halutaan ainoastaan kuunnella. Linux Mint -käyttöjärjestelmälle asennettuna Wireshark on lähestulkoon täysin saman näköinen kuin kuvassa 7 Windows 8.1 –käyttöjärjestelmälle asennettuna.



KUVA 8. Wireshark-näkymä .pcapng-tiedosto avattuna

Kuvassa 8 avatun tiedoston sisältämässä liikenteessä on jonkin verran epätoivottua liikennettä, jota on aiheuttanut kannettava tietokone sekä protokolla-analysaattori. Esimerkkitallenne on tilanteesta, jossa DUT on kytkeytyneenä 3G-verkkoon. Tässä tapauk-

sessa olisi toivottua suodattaa liikenne niin, että jäljelle jää ainoastaan DUT:n aiheuttama liikenne.



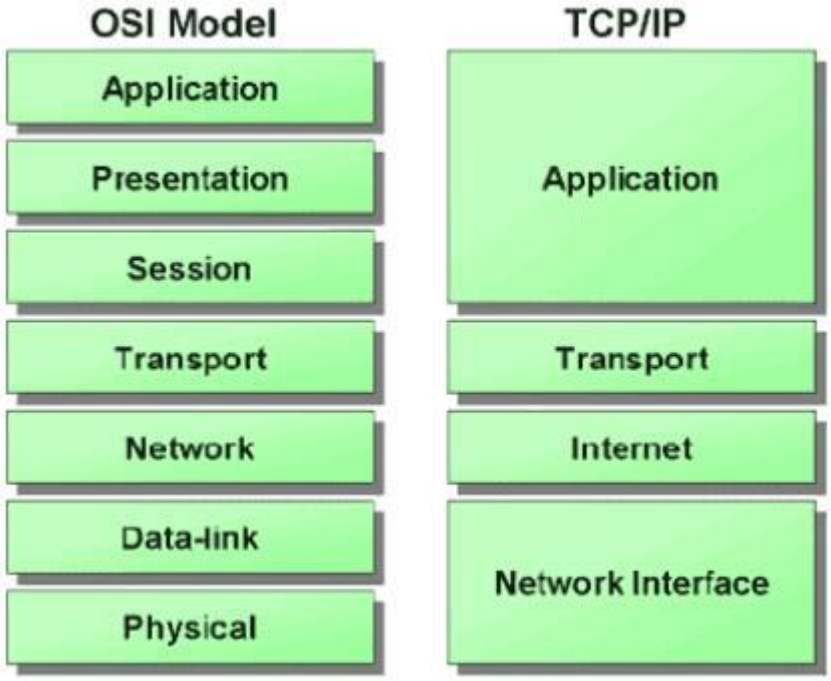
KUVA 9. Wiresharkin suodatintoiminto

Kuvassa 9 ympyröityyn kenttään on syötetty suodatusehtoja. Ehtona on ”**ip.addr == 192.168.43.220 && ip && tcp**”, joka tarkoittaa, että ainoastaan kyseisen IP-osoitteen TCP/IP-liikenne näytetään. Mitä tahansa muutakin suodatustoimintoa voidaan käyttää, jotta saadaan haluttu tulos.

3 HAVAITUT PROTOKOLLAT

Tässä kappaleessa käsitellään lyhyesti kaikki ne tietoliikenneprotokollat, joita kohdattiin Wiresharkin .pcapng–tiedostoista eli dumpeista eri älylaitteiden IP-osoitteiden perusteella. Protokollien perusteellinen käsittely on tämän työn puitteissa mahdotonta, koska jokaisesta voisi erikseen pitää oman esitelmänsä.

Kaikki tässä työssä kohdatut protokollat kuuluvat TCP/IP-protokollapinoon. TCP/IP-protokollapino on yhdistelmä useista protokollista, joita käytetään internet–liikennöinnissä. TCP/IP sisältää hyvin paljon monia muitakin protokollia tässä työssä kohdattujen lisäksi. Se toimii viidellä eri OSI-mallin (Open Systems Interconnection) kerroksella.



KUVA 10. TCP/IP ja OSI-malli http://www.techexams.net

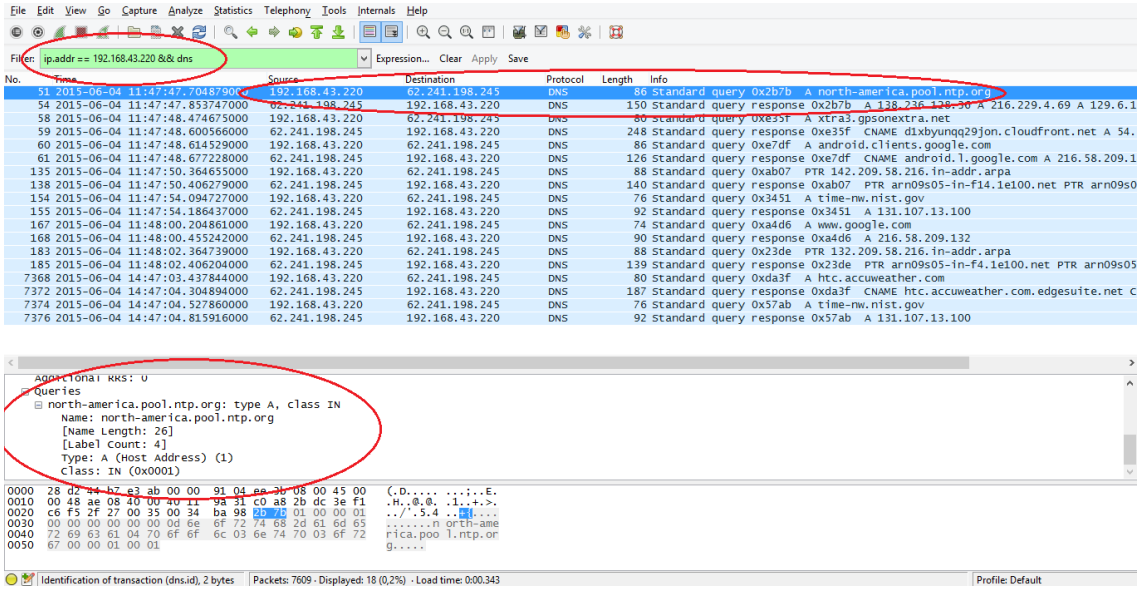
Kuvassa 10 on rinnastettu OSI-mallin sekä TCP/IP:n toisiaan vastaavat kerrokset.

3.1 DNS

DNS (Domain Name System) on protokolla, jonka avulla saadaan tiettyä domain-nimeä vastaava IP-osoite selville jatkotoimenpiteitä varten. On helpompi muistaa IP-osoitteiden sijaan sivustojen nimiä kuten esimerkiksi www.google.com. Kun halutaan

palvelimen nimen perusteella ottaa yhteys johonkin, DNS-palvelimelle lähtee DNS-kysely liittyen annettuun domain-nimeen. DNS-palvelin vastaa kyselyyn ilmoittamalla, mitä IP-osoitetta annettu domain-nimi vastaa. Tämän annetun IP–osoitteen perusteella voidaan muodostaa yhteys haluttuun kohteeseen.

DNS-kyselyiden perusteella voidaan hieman arvuutella, että minkä nimisiin osoitteisiin DUT:lla on aikomus muodostaa yhteys. Aluksi käsitellään esimerkinomaisesti yhden DUT:n DNS-liikennöinti ja käsitellään siihen sisältyviä toiminnallisuuksia. Kaikkien laitteiden dumppeja on turha erikseen käsitellä yksityiskohtaisesti ja kuvallisesti, koska kaikissa tapauksissa toiminnallisuus on periaatteessa täsmälleen sama, sisältö vain saattaa olla eri.



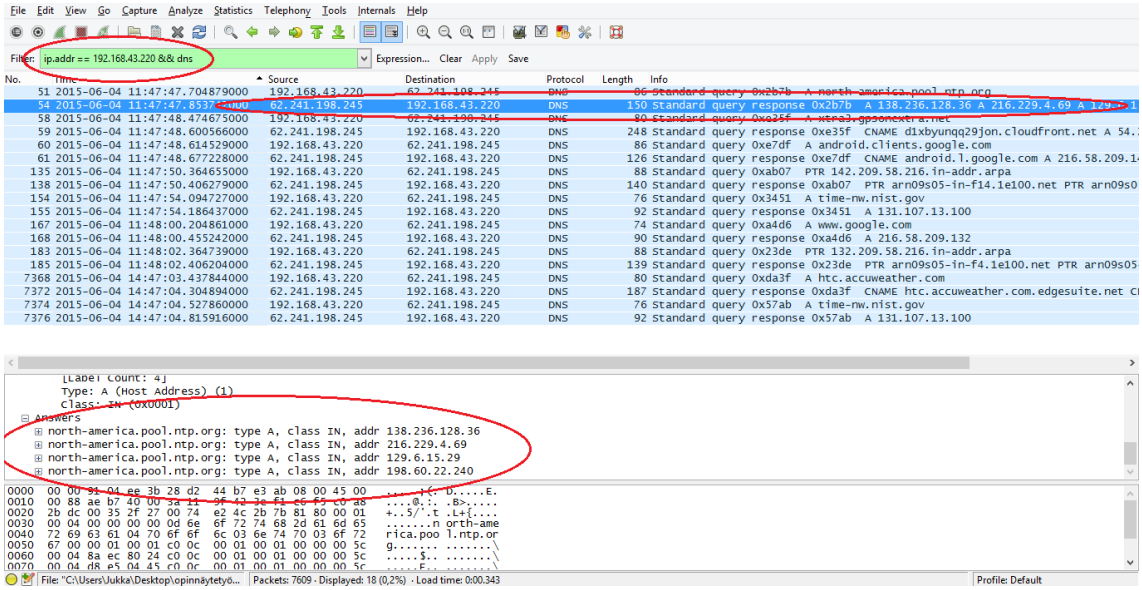
KUVA 11. Yhden DUT:n DNS-kyselyt 3G-verkkoon kytkeytyneenä

Kuvassa 11 on HTC Desire -älypuhelimen tuottamaa tietoliikennedataa. Vasemmassa yläkulmassa punaisella ympyröitynä ovat käytetyt suodatustoiminnot ”**ip.addr == 192.168.43.220 && dns**”, joista ”**ip.addr == 192.168.43.220**” tarkoittaa sitä, että vain kyseiseen IP-osoitteeseen liittyvää dataa esitetään. ”**&&**” tarkoittaa, että suodatustoiminnan syötteeseen tulee vielä joitakin lisäehtoja. ”**dns**” tarkoittaa, että pelkästään DNS-kyselyt esitetään.

Kuvan 11 keskellä ylhäällä oleva leveämpi ympyröinti osoittaa tässä tapauksessa valittua datapakettia, joka on tuotu esiin korostetulla sinisellä värillä. Kyseisellä rivillä näkyy lähde- sekä kohdeosoitteet, käytetty protokolla, datapaketin koko sekä infokenttä.

Tässä tapauksessa lähdeosoite on DUT:n IP-osoite ”**192.168.43.220**”, kohdeosoite on DNA:n DNS-palvelimen IP-osoite ”**62.241.198.245**”, käytetty protokolla on ”**DNS**” sekä infokentästä näkyy Domain-nimi ”**north-america.pool.ntp.org**”, jonka IP-osoitteen DUT haluaa tietää.

Kuvan 11 vasemmassa alareunassa oleva ympyröinti osoittaa datapaketista avattua tarkempaa sisältöä, josta on valittu tässä tapauksessa ”**Domain Name System**” ja sen alavalikko ”**Query**”. Kyseisen paketin sisällöstä selviää myös sama DNS-kyselyn kohteena oleva domain-nimi ”**north-america.pool.ntp.org**”.

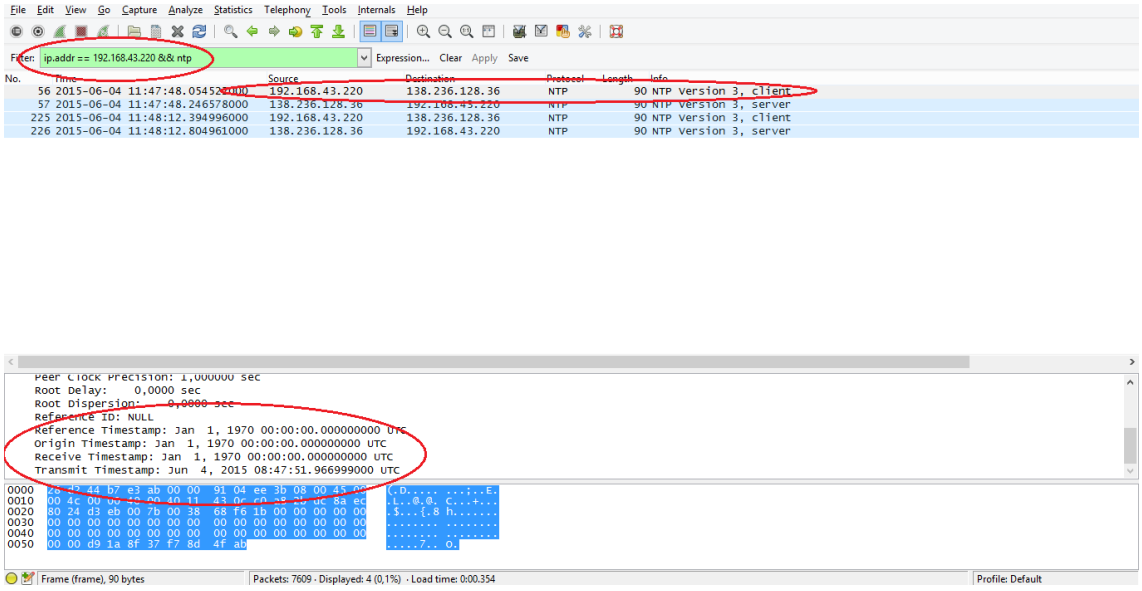


KUVA 12. DUT:n DNS-vastaukset 3G-verkkoon kytkeytyneenä

Kuvassa 12 vasemmassa yläkulmassa on ympyröity samat suodatustoiminnon ehdot kuin edellisessäkin tilanteessa. Keskellä ylhäällä lähde- sekä kohdeosoitteet ovat samat kuin edellisessä tilanteessa, mutta toisin päin, koska kyseessä on vastaus (response) DUT:n tekemään kyselyyn (query). Vasemmalla alhaalla oleva ympyröinti osoittaa datapaketin sisältämää tarkempaa tietoa DNS-vastauksesta. Datapaketin Domain Name System-kohdan alavalikosta Answers-kohta sisältää haluttua Domain-osoitetta vastaavat IP-osoitteet. Tässä tapauksessa ”**north-america.pool.ntp.org**” –osoitetta vastaa neljä eri IP-osoitetta, jotka ovat ”**138.236.128.36, 216.229.4.69, 129.6.15.29 ja 198.60.22.240**”. Domain nimen perusteella on mahdollista yrittää tehdä jonkinlaisia johtopäätöksiä, mutta näiden osoitteiden tarkempaa alkuperää voidaan selvittää syöttämällä ne yksitellen esimerkiksi Googlen hakukoneeseen.

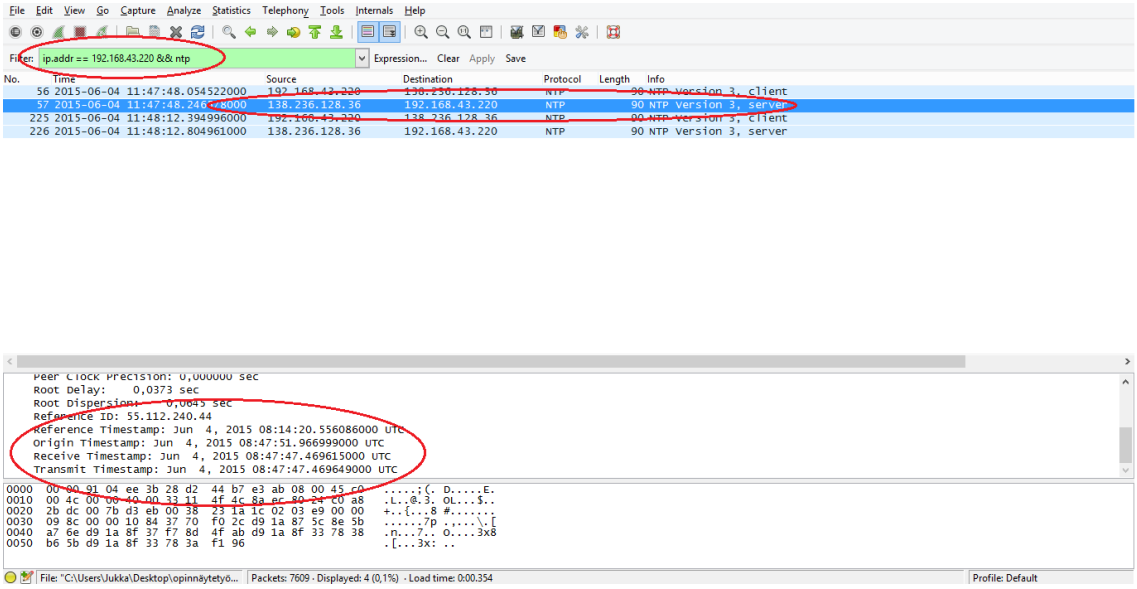
3.2 NTP

NTP (Network Time Protocol) on protokolla, jota käytetään täsmällisen aikatiedon välittämiseksi tietokoneiden välille eli siis synkronointiin. NTP-palvelimien tarjoama aikatieto on teoriassa nanosekuntien suuruusluokkaa.



KUVA 13. DUT:n tietoliikenteestä poimittua NTP-dataa

Kuvassa 13 vasemmassa yläkulmassa on ympyröitynä suodatustoiminnon suodatusehdot, jotka ovat tässä tapauksessa ”**ip.addr == 192.168.43.220 && ntp**”. Tällä suodatuksella saadaan DUT:lle kuuluvaan IP-osoitteeseen liittyen kaikki tietoliikenne, joka liittyy NTP-protokollaan. Keskellä ylhäällä oleva ympyröinti sisältää lähde- sekä kohdeosoitteet ”**192.168.43.220**” ja ”**138.236.128.36**” ja käytetty protokolla ”**NTP**”. 192.168.43.220 on siis DUT:n IP-osoite ja 138.236.128.36 on NTP-palvelimen osoite. DUT kysyy NTP-palvelimelta tarkkaa kellonaikaa. DUT:n lähettämä datapaketti sisältää DUT:n oman kellonajan, joka näkyy kuvan 13 vasemmassa alakulmassa ympyröitynä.



KUVA 14. NTP-palvelimen vastaus DUT:lle

Kuvassa 14 käytetään edelleen samaa suodatustoimintoa kuin edellisessäkin tilanteessa. Lähde- sekä kohdeosoitteet ovat luonnollisesti samat, mutta päinvastoin, koska kyseessä on NTP-palvelimen vastaus DUT:n kyselyyn. Kuvan vasemmassa alalaidassa näkyy NTP-palvelimen lähettämän datapaketin sisältö. ”**Reference Timestamp**” on se paikallinen aika, jolloin paikallinen kello on asetettu tai korjattu, ja tämän aikaleiman client asettaa itselleen. ”**Origin Timestamp**” on paikallinen aika, jolloin client lähetti pyynnön. ”**Receive Timestamp**” on paikallinen aika jolloin palvelin on vastaanottanut pyynnön**.** ”**Transmit Timestamp**” on paikallinen aika, jolloin palvelin on lähettänyt vastauksen pyyntöön.

3.3 TCP

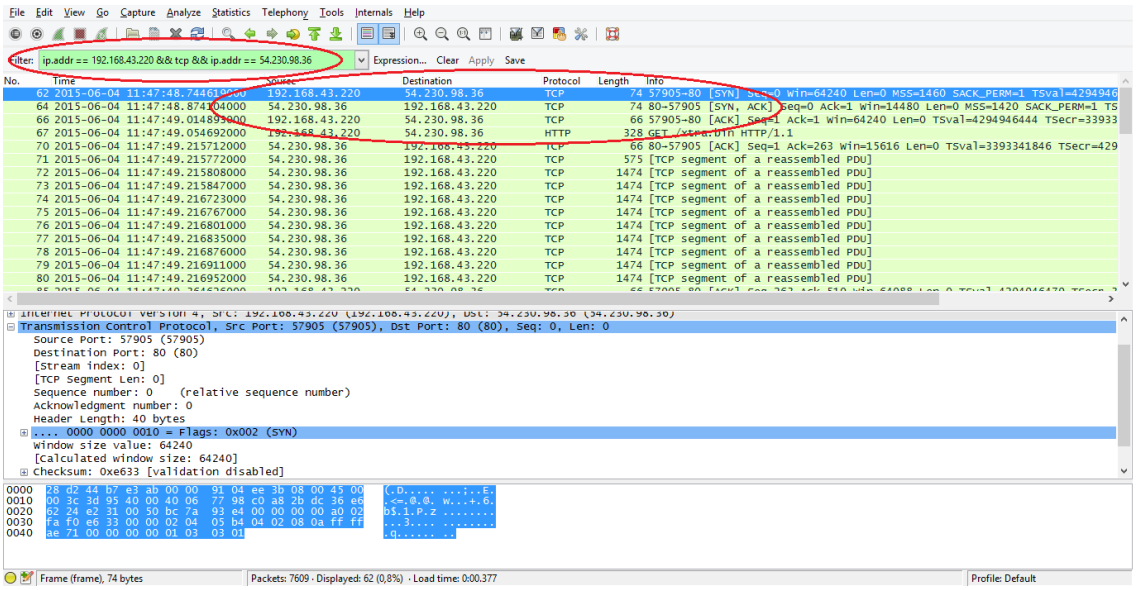
TCP (Transmission Control Protocol) on protokolla, jonka avulla luodaan yhteyksiä internetiin yhteydessä olevien tietokoneiden välille tiedonsiirtoa varten. TCP:n avulla tietokoneet voivat lähettää toisilleen tavujonoja luotettavasti sen sisältämien tarkistus- sekä uudelleenlähetystoimintojen avulla. Protokolla huolehtii myös siitä, että paketit saapuvat perille oikeassa järjestyksessä. Vastaanottaja kuittaa paketin saaduksi ja ilmoittaa, mitä pakettia odottaa seuraavaksi. Vioittunut tai hukkunut paketti voidaan lähettää uudestaan.

TCP-yhteys muodostetaan ns. kolmitiekättelyllä. Kolmitiekättelyssä aloittaja lähettää ensin kohteelle SYN-paketin. Kohteen vastaanotettua SYN-paketti, vastaa se aloittajalle

SYN/ACK-paketilla osoituksena siitä, että aloittajan lähettämä SYN-paketti on saapunut perille. Lopuksi aloittaja vastaa kohteelle vielä ACK-paketilla merkiksi siitä, että on vastaanottanut kohteen lähettämän SYN/ACK-paketin.

Itse tiedonsiirtovaiheessa datan eheys varmistetaan usealla eri tavalla kuten sekvenssinumeroinnilla, tarkistussummilla sekä hukattujen pakettien ajastimilla ja tunnistimilla. Jokainen paketti kuitataan vastaanotetuksi, ja mikäli kuittausta ei tule, lähetetään paketti uudestaan.

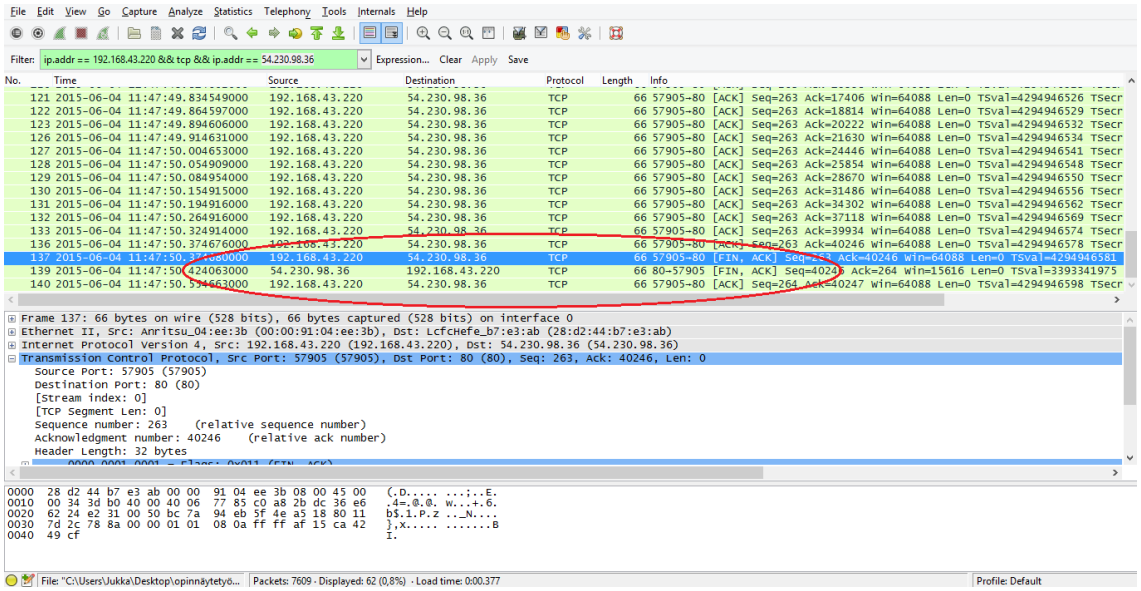
Yhteyden päättämiseen on kolme tapaa. Ensimmäinen tapa on, että tiedonsiirron päätyttyä yhteys päätetään nelitiekättelyllä. Molemmat osapuolet lähettävät FIN-paketin sekä kuittaavat toistensa FIN-paketit ACK-paketilla. Toinen tapa on, että yhteys päätetään kolmitiekättelyllä, jossa ensimmäinen osapuoli lähettää FIN-paketin ja toinen osapuoli kuittaa tämän FIN-ACK-paketilla. Lopuksi ensimmäinen osapuoli vielä lähettää ACK-paketin. Yhteys voidaan myös katkaista niin, että jompikumpi osapuoli lähettää RESET-lipulla varustetun paketin. Toimenpiteellä yhteys katkaistaan heti ilman mitään vastauspaketteja.



KUVA 15. DUT:n TCP-istunnon aloittaminen

Kuvassa 15 on käytetty suodatustoiminnossa ehtona ”**ip.addr == 192.168.43.220 && tcp && ip.addr == 54.230.98.36**”. Tämän ehdon avulla on liikenteestä suodatettu jäljelle vain kahden eri IP-osoitteen välinen TCP-liikenne. Toinen IP-osoite on DUT:n ja toinen on toistaiseksi tuntematon IP-osoite. Tässä tapauksessa DUT haluaa joltakin

www-palvelimelta jotakin sisältöä HTTP (Hyper Text Transfer Protocol) –protokollan avulla. Kuvassa 15 keskellä ylhäällä on ympyröity kolmitiekättelyn tapahtumat. Ensin DUT lähettää kohteelle SYN-paketin, johon kohde vastaa SYN/ACK-paketilla. Lopuksi DUT vielä kuittaa saaneensa SYN/ACK-paketin lähettämällä ACK-paketin. Tämän jälkeen voidaan aloittaa istunto tiedonsiirtoa varten.

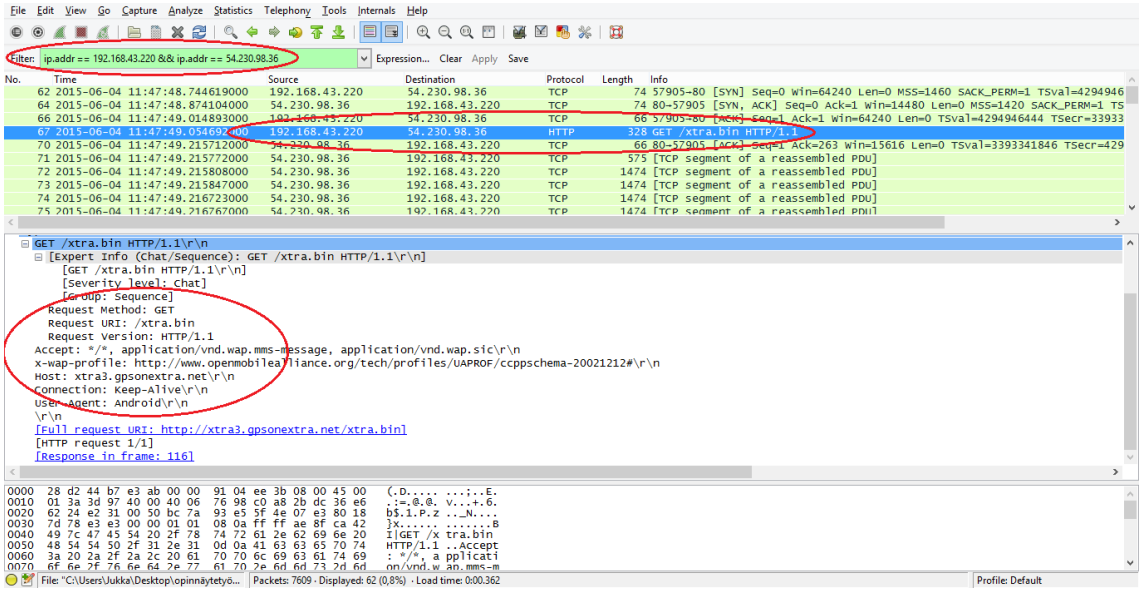


KUVA 16. TCP-istunnon päättäminen

Kuvassa 16 on ympyröity se osa liikenteestä, jossa voidaan havaita tapahtuvan TCP-istunnon päättäminen. DUT lähettää paketin joka sisältää FIN-lipun ja johon kohde vastaa FIN/ACK-paketilla. Lopuksi DUT vielä kuittaa saaneensa FIN/ACK-paketin lähettämällä ACK-paketin. Joissakin tapauksissa yksi paketti saattaa sisältää useampia lippuja, kuten kuvassa 16 sinisellä korostetussa paketissa huomataan. Se sisältää sekä ACK-kuittauksen viimeisestä paketista ja FIN-lipun osoituksena siitä, että istunto on valmis päätettäväksi.

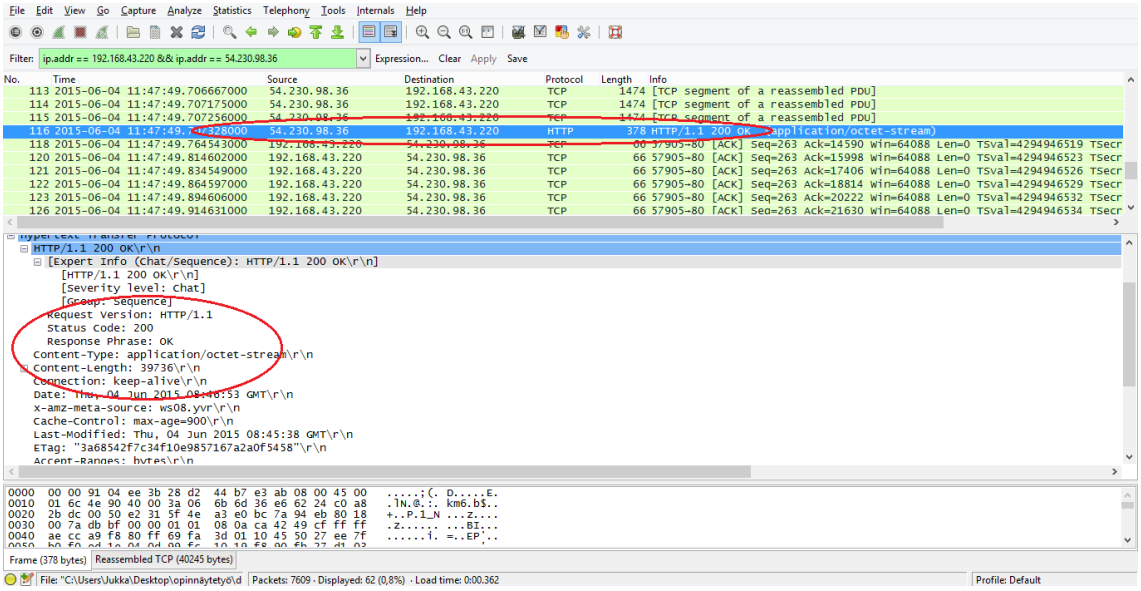
3.4 HTTP

HTTP (Hyper Text Transfer Protocol) on protokolla selainten sekä www-palvelimien tiedonsiirtoon. Lyhyesti sanottuna protokolla toimii niin, että käyttäjä (client) avaa TCP-yhteyden palvelimen kanssa ja lähettää HTTP GET -pyynnön. Palvelin vastaa lähettämällä sopivaa dataa, joka voi olla mm. kuvia, ohjelmia tai ääntä. Käyttäjä voi myös lähettää HTTP POST –pyynnön, johon käyttäjä voi sisällyttää jotakin tietoa lähetettäväksi palvelimelle.



KUVA 17. DUT:n lähettämä HTTP GET –pyyntö

Kuvassa 17 on suodatustoiminnolla rajattu liikenne niin, että ainoastaan DUT:n sekä toisen tuntemattoman IP-osoitteen liikenne näytetään. Kuvassa keskellä ylhäällä ympyröidyssä kehyksessä lähdeosoitteena on 192.168.43.220, joka on DUT:n IP-osoite sekä kohdeosoitteena on 54.230.98.36, johon HTTP GET –pyyntö lähetetään. Tätä HTTP GET –pyyntöä edeltää TCP-istunnon aloittaminen kolmitiekättelyllä, joka näkyy kuvassa sinisellä korostetun HTTP GET –pyynnön yläpuolella. GET-pyynnön sisältämää dataa aletaan siirtää TCP-protokollan avulla. Alempana ympyröity kohta sisältää pyynnön tyypin ”**Request Method: GET**”, pyyntöä koskevan URI:n (Uniform Resource Identifier) ”**Request URI: /xtra.bin**” sekä pyynnössä käytetty HTTP-versio ”**Request Version: HTTP/1.1**”. Samasta tietokentästä selviää myös kohdeosoitteen IP-osoitetta vastaava Domain-nimi ”**host: xtra3.gpsonextra.net**”.

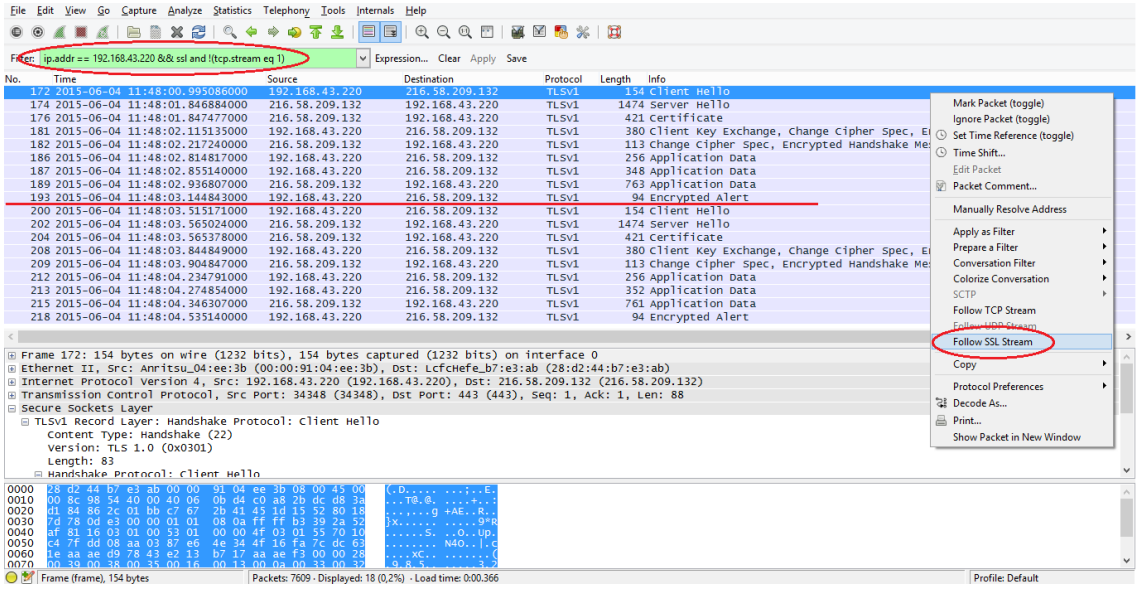


KUVA 18. Palvelin ilmoittaa onnistuneesta HTTP-vastauksesta

Kuvassa 18 ylhäällä keskellä ympyröity kehys, jossa palvelin lähettää HTTP OK –vastauksen. Vasemmalla alhaalla ympyröidyssä tietokentässä ”**Response Phrase: OK**” tarkoittaa onnistunutta vastausta pyyntöön.

3.5 TLS

TLS (Transport Layer Security) on protokolla, jolla on kaksi tarkoitusta, joista toinen on datan salaaminen ja toinen on tunnistautuminen.Kyseinen protokolla on aiemmin tunnettu myös nimellä SSL (Secure Sockets Layer). Arkaluontoista dataa lähetettäessä on toivottavaa, että data salataan eli kryptataan erilaisten monimutkaisten menetelmien avulla. Tämäntyyppinen data voisi olla esimerkiksi luottokorttitiedot, henkilötiedot ja salasanat yms. On myös toivottavaa, että kohde, jonka kanssa dataa lähetetään, on juuri se, joksi sitä luullaan, ja siihen tarpeeseen tulee tunnistautuminen. TLS-istunnon alussa käyttäjä (client) sekä palvelin (server) vaihtavat keskenään tarvittavia tietoja istunnon aloittamista varten. Näitä tietoja ovat mm. kryptausmenetelmä, SSL-sertifikaatti ja sen voimassaoloaika, käytettävä TLS-versio, satunnaisluku sekä pakkausmenetelmä. Käytännössä käyttäjä kertoo ensin, mitä kaikkia tekniikoita se tukee, ja palvelin valitsee näistä sopivimmat.



KUVA 19. TLS-istunto

Kuvassa 19 on kaksi identtistä TLS-istuntoa, jotka on erotettu punaisella viivalla. Haluttua TLS-istuntoa voi seurata painamalla hiiren oikeaa näppäintä ensimmäisen TLS-kehyksen kohdalla ja valitsemalla ”**Follow SSL Stream**”. Tästä syystä vasemmassa yläkulmassa olevaan ympyröityyn suodatustoimintoon lisääntyy ” **and !(tcp.stream eq 1)**” –ehto. Kuvasta on hieman vaikea todentaa kaikki protokollan mukaiset tapahtumat, koska yksi paketti saattaa sisältää useamman eri lipun (Samassa paketissa esim. **Client Key Exchange**+**Change Cipher Spec**+**Encrypted Handshake Message**). Encrypted Handshake Message tarkoittaa samaa kuin Finished-lippu.

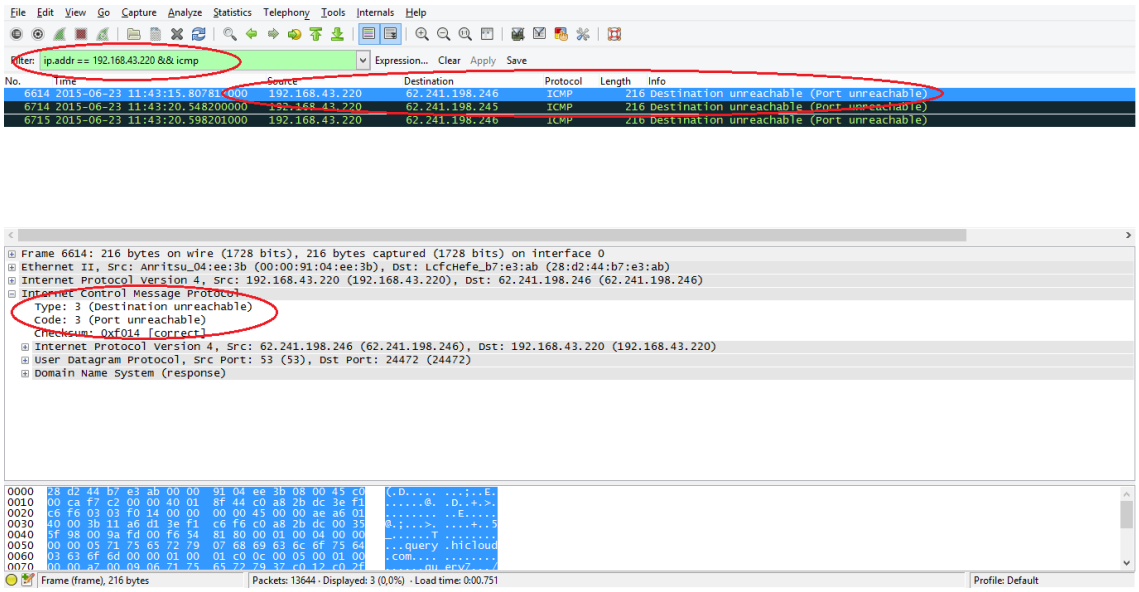
Istunnon kulku etenee seuraavanlaisesti:

- Client lähettää ”**ClientHello**” –viestin, joka sisältää tiedot tekniikoista, joita se tukee kuten TLS-protokollan versionumeron, satunnaisluvun ja listan salaus- sekä pakkaustekniikoista.
- Server vastaa ”**ServerHello**” –viestillä, jossa se ilmoittaa valitut tekniikat clientin tarjoamista vaihtoehdoista.
- Server lähettää ”**Certificate**” –viestin, joka sisältää tietoa sen sertifikaatista sekä sen voimassaoloajasta.
- Server lähettää ”**ServerHelloDone**” –viestin, joka tarkoittaa sitä, että sen puolesta kättelyneuvottelu on valmis.
- Client lähettää ”**ClientKeyExchange**” –viestin, joka saattaa sisältää julkisen avaimen, riippuen siitä mitä salaustekniikkaa on päädytty käyttämään.
- Client lähettää ”**ChangeCipherSpec**” –viestin, jossa se kertoo serverille alkavansa lähettää kryptattua dataa.

- Lopuksi client lähettää ”**Finished**” –viestin, joka sisältää suolan (hash) sekä viestin autentikointikoodin. Server yrittää dekryptata clientin ”**Finished**” –viestiä ja vahvistaa, että suola sekä autentikointikoodi ovat oikeat.
- Lopuksi server lähettää ”**ChangeCipherSpec**” –viestin, joka kertoo clientille alkavansa lähettää kryptattua dataa. Server lähettää vielä ”**Finished**” –viestin, jonka avulla client voi puolestaan vahvistaa suolan sekä autentikointikoodin oikeellisuuden.
- ”**Application Data**” –viestit sisältävät varsinaista salattua dataa eli hyötykuormaa.
- ”**Encryption Alert**” –viestit tarkoittavat tässä tapauksessa sitä, että client kertoo yhteyden sulkemisesta kun haluttu data on siirretty.

3.6 ICMP

ICMP (Internet Control Message Protocol) on protokolla, jonka avulla verkkolaitteet lähettävät mm. virheilmoituksia ja muuta tietoa liittyen verkon toimintaan. Sitä voidaan myös käyttää Ping- tai Traceroute-toiminnon avulla selvittämään verkon viiveitä (Delay) tai hyppyjen (Hops) määrää. Tässä kappaleessa esitellään tämän työn puitteissa tapahtuvaa ICMP-liikennettä.



KUVA 20. DUT:n lähettämiä ICMP-paketteja

Kuvassa 20 suodatintoiminnon ehtoina on käytetty DUT:n IP-osoitetta sekä ICMP-protokollaa, ” **ip.addr == 192.168.43.220 && icmp**”. Kuvan keskellä ylhäällä on sinisellä korostettu ja punaisella ympyröity tutkittava paketti, josta selviää lähde- sekä kohdeosoitteet, käytetty protokolla sekä tietoa paketin sisällöstä. Lähdeosoite on DUT:n IP-

osoite sekä kohdeosoite on DNA:n DNS-palvelimen IP-osoite. DUT siis ilmoittaa DNS-palvelimelle epäonnistuneesta yhteydestä. Kuvassa vasemmalla alakulmassa ympyröidyssä tietokentässä on tiedot ”**Type: 3 (Destination unreachable)**” sekä ”**Code: 3 (Port Unreachable)**”. Niistä voidaan saada hieman tietoa siitä miksi paketti on hävitetty.

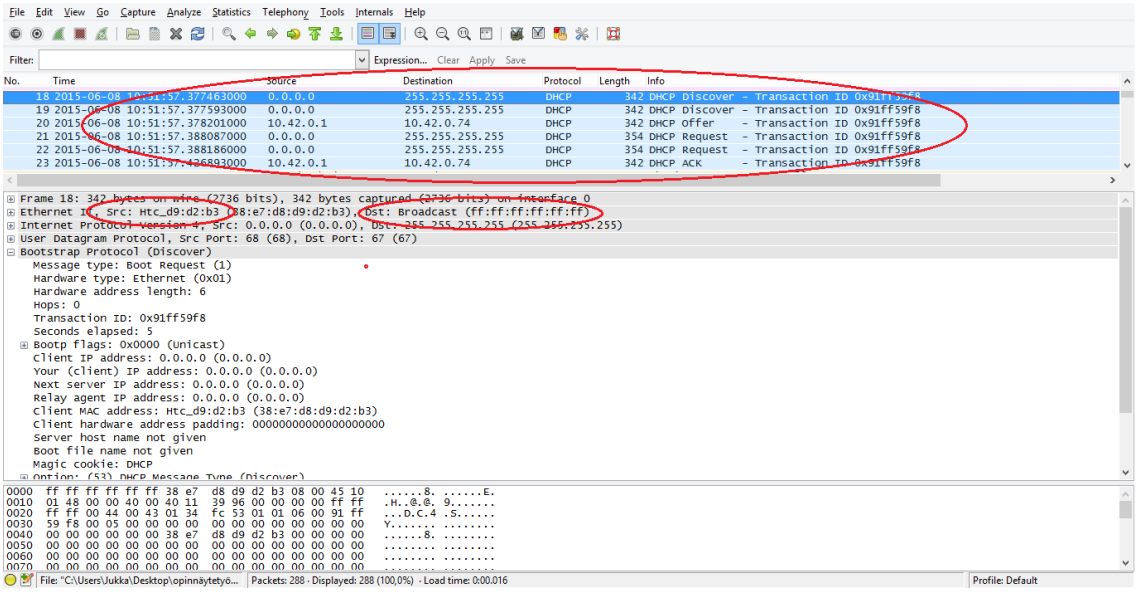
”**Destination unreachable**” tarkoittaa sitä, että kyseinen paketti on hävitetty, koska se ei ole saavuttanut lopullista määränpäätään. Tämä voi johtua monestakin asiasta kuten verkon ongelmista tai siitä, että kohdelaitteella ei ole ollut resursseja käsitellä pakettia.

”**Port unreachable**” puolestaan tarkoittaa sitä, että:

1. Kyseinen paketti on reititetty onnistuneesti perille.
2. Näiden kahden kohteen välinen viimeinen reititin on tehnyt ARP-kyselyn ja on sen perusteella lähettänyt paketin kohteeseen.
3. Kohde on ollut online-tilassa ja valmis vastaanottamaan paketin välimuistiinsa.
4. Paketti on prosessoitu jollekin tietylle protokollalle ja se on yritetty lähettää kohteelle tiettyyn porttiin.
5. Kohteen porttia ei ole jostain syystä saavutettu.

3.7 DHCP

DHCP (Dynamic Host Configuration Protocol) on protokolla, jota käytetään IP-osoitteiden jakamiseen lähiverkossa. DHCP-palvelimella on tietty IP-osoiteavaruus eli pooli, josta se jakaa käytettävissä olevia osoitteita verkon laitteille. Annettu osoite on voimassa ennalta määritetyn ajan. DHCP-palvelin voi jakaa verkon laitteille tiedoksi myös oletusyhdyskäytävän tai DNS-palvelimien IP-osoitteita. DHCP-protokolla ei reitity muualle internetiin, vaan sitä käytetään vain aina kulloisessakin lähiverkossa.



KUVA 21. IP-osoitteen pyytäminen ja myöntäminen DHCP:llä

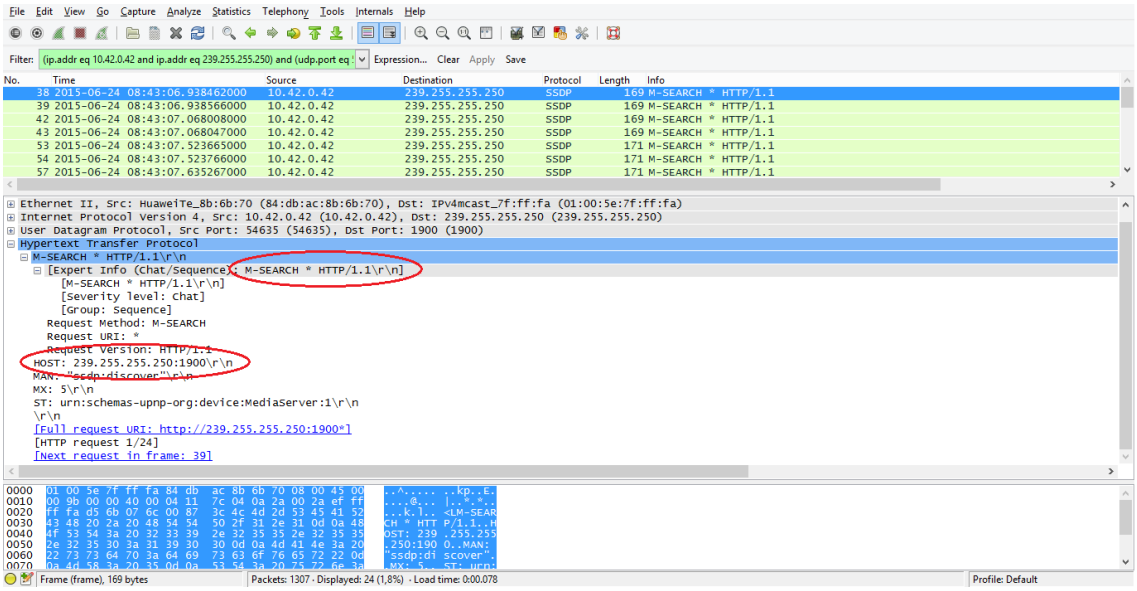
Kuvassa 21 sinisellä korostettu paketti on DUT:n lähettämä ”**DHCP Discover”** -pyyntö. Tuntemattomasta syystä tämä pyyntö tapahtuu kaksi kertaa peräkkäin. Vasemmalla alempana ympyröidystä kohdasta selviää tarkempaa tietoa paketista ja että kyseessä on HTC Desire –älypuhelimen MAC-osoite ”**Src: Htc_d9:d2:b3**”, josta kyseinen paketti on lähtöisin. Kuvan keskellä pienellä ympyröity osio kertoo kohteen, johon kyseinen ”**DHCP Discover**” –pyyntö on lähetetty ja kyseessä on ns. broadcast lähetys ”**Dst: Broadcast: (ff:ff:ff:ff:ff:ff)**”, joka lähetetään verkon kaikille laitteille koska pyynnön tekijä ei tiedä kuka tai missä DHCP-palvelin on. Kyseistä pakettia alempana on seuraavana DHCP-palvelimen tekemä ”**DHCP Offer**” –paketti, jossa DHCP-palvelin tarjoaa jotakin tiettyä IP-osoitetta DUT:lle. DHCP-palvelimena toimii tässä tapauksessa Wireless Access Point -sovellus, joka on muodostettu kannettavan tietokoneen Linux Mint –käyttöjärjestelmällä. Seuraavaksi DUT lähettää ”**DHCP Request**” –paketin, joka tarkoittaa, että DUT on halukas ottamaan käyttöön tarjotun IP –osoitteen. Tämän jälkeen DHCP-palvelin kuittaa IP-osoitteen myönnetyksi ”**DHCP ACK**” –paketilla.

3.8 SSDP

SSDP (Simple Service Discovery Protocol) on protokolla, jota käytetään Plug & Play –palveluiden tai laitteiden löytämiseen sekä mainostamiseen. SSDP käyttää Unicast-osoitteita kyselyihin vastaamiseen sekä Multicast-osoitetta 239.255.255.250 ja porttia 1900 kyselyiden tekemiseen. SSDP:tä voidaan käyttää molempien IPv4- sekä IPv6-

protokollien päällä. SSDP kuuluu UpnP-protokollapinoon (Universal Plug and Play) ja se käyttää datan siirtämiseen UDP-protokollaa (User Datagram Protocol).

SSDP käyttää NOTIFY-metodia ilmoittaakseen tietoja palvelun saatavuudesta tai saamattomuudesta Multicast-ryhmälle. Käyttäjä (client), joka haluaa tietoja saatavilla olevista palveluista verkossa käyttää M-SEARCH-metodia.Tällaisiin kyselyihin lähetetään vastaukset Unicast-lähetyksenä osoitteeseen sekä porttiin, josta alkuperäinen kysely tuli.



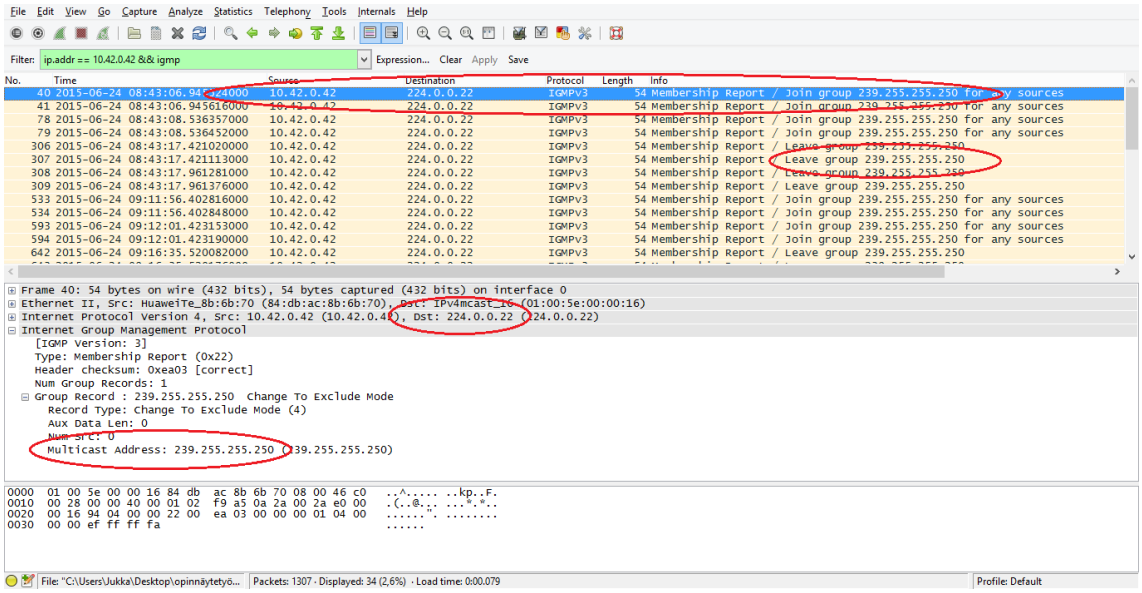
KUVA 22. DUT:n tekemiä SSDP M-SEARCH –kyselyitä

Kuvassa 22 on suodatettu esille DUT:n tekemiä SSDP-kyselyitä. Sinisellä korostettu paketti sisältää tarkempaa tietoa sisällöstä, jotka on ympyröity punaisella. Ylempi ympyröinti ”**M-SEARCH * HTTP/1.1\r\n**” sisältää tiedon käytetystä metodista M-SEARCH sekä DUT:n tukemasta HTTP-protokollan versiosta 1.1. Vasemmalla alempana ympyröity kohta ”**HOST: 239.255.255.250:1900**” sisältää tiedon kohteesta, joka on Multicast IP -osoite sekä käytettävästä portista, joka on 1900. Kuvan 22 tilanteen suodatusehdoilla ei havaita vastauksia pyyntöihin, koska ne lähetetään Unicast-lähetyksenä jostakin tietystä IP-osoitteesta.

3.9 IGMP

IGMPv3 (Internet Group Management Protocol version 3) on protokolla, jolla voidaan dynaamisesti muodostaa tai hallinnoida Multicast-istuntoja IPv4-verkoissa. Verkon laite lähettää 224.0.0.22 Multicast –osoitteeseen paketin, jolla kerrotaan tietoja jostakin Multicast-istunnosta tai halutaan tietoa jostakin toisesta tietystä Multicast-istunnosta. Multi-

cast-istunnot voivat olla mm. videoneuvotteluja tai IPTV-lähetyksiä (Internet Protocol Television). Verkkolaitteet kuten reitittimet sekä kytkimet käyttävät IGMP:tä Multicast-ryhmien hallitsemiseen.



KUVA 23. DUT:n lähettämiä IGMPv3-paketteja

Kuvassa 23 on sinisellä korostettu sekä punaisella ympyröity DUT:n lähettämä IGMPv3-paketti. Kuvassa keskellä ympyröity kohta ”**Dst: 224.0.0.22**” on IGMPv3:n oma Multicast-osoite johon DUT lähettää pyyntönsä liittyä erääseen toiseen Multicast-ryhmään, joka on kuvan vasemmassa alareunassa ympyröitynä ”**Multicast Address: 239.255.255.250 (239.255.255.250)**”. Kuvan oikeassa reunassa pienempi ympyröinti osoittaa DUT:n lähettämän erään toisen paketin infokentästä tiedon, että DUT ilmoittaa poistuvansa 239.255.255.250 Multicast –ryhmästä, johon se aiemmin liittyi.

4 VARSINAISEN DATAN ANALYSOINTI

Tässä kappaleessa käsitellään ja spekuloidaan, miksi älylaitteet olivat yhteydessä joihinkin palvelimiin kytkeytyneenä 3G-verkkoon sekä WLAN-verkkoon. Liitteenä olevissa mittauspöytäkirjoissa kerrotaan kaikki selville saadut tiedot mitä kunkin IP-osoitteen perusteella saatiin selville. Liitteenä olevien mittauspöytäkirjojen IP-osoitteiden alkuperän selvittämiseen käytettiin Googlen hakukonetta. On olemassa useita sivustoja, kuten **https://ipinfo.io, http://www.ip-tracker.org, https://geoiptool.com** ja **http://tools.tracemyip.org**, jotka pystyvät mahdollisesti kertomaan annetun IP-osoitteen perusteella muun muassa seuraavaa:

-mille palveluntarjoajalle (ISP, Internet Service Provider) kyseinen osoite kuuluu
-millä aikavyöhykkeellä kyseinen osoite sijaitsee
-maan ja maanosan missä kyseinen osoite sijaitsee
-kaupungin missä kyseinen osoite sijaitsee
-omistajan fyysisen osoitteen
-maan missä omistaja sijaitsee
-omistajan puhelinnumeron
-omistajan omat nettisivut
-hostin eli palvelimen URI:n

Kappaleessa sivuutetaan joihinkin protokolliin liittyviä itsestäänselvyyksiä, joita ovat mm. DNS-kyselyt DNS-palvelimille sekä NTP-kyselyt NTP-palvelimille.

4.1 HTC Desire

Laitteen tarkemmat tekniset tiedot saatiin laitteen IMEI-koodin (International Mobile Equipment Identity) perusteella **http://www.imei.info** –sivustolta. Alla olevat tiedot on kopioitu suoraan mainitulta sivuilta sellaisenaan.

Basic information:

Device type:	Phone
Design:	Classic
Released:	2010 r.
SIM card size:	Mini Sim - Regular
GSM:	✔850 900 1800 1900
HSDPA:	✔900 2100
Dimensions (H/L/W):	119 x 60 x 11.9 mm, vol. 84 cm³
Display:	AMOLED Color (16M) 480x800px (3.7")
Touch screen:	✔
Weight:	135 g
Time GSM (talk/stand-by):	6.6 / 340 hrs. (14.2d)
Time UMTS (talk/stand-by):	6.5 / 360 hrs. (15.0d)
Battery:	Li-Ion 1400 mAh
Built-in memory:	✔512 MB
Memory card:	✔MicroSD max. 32 GB
OS:	Android 2.1
CPU type:	Snapdragon QSD8250
CPU freq.:	1000.0 MHz
QWERTY keyboard:	✖

KUVA 24. Kartta palvelimista joihin Htc Desire -älylaite otti yhteyttä

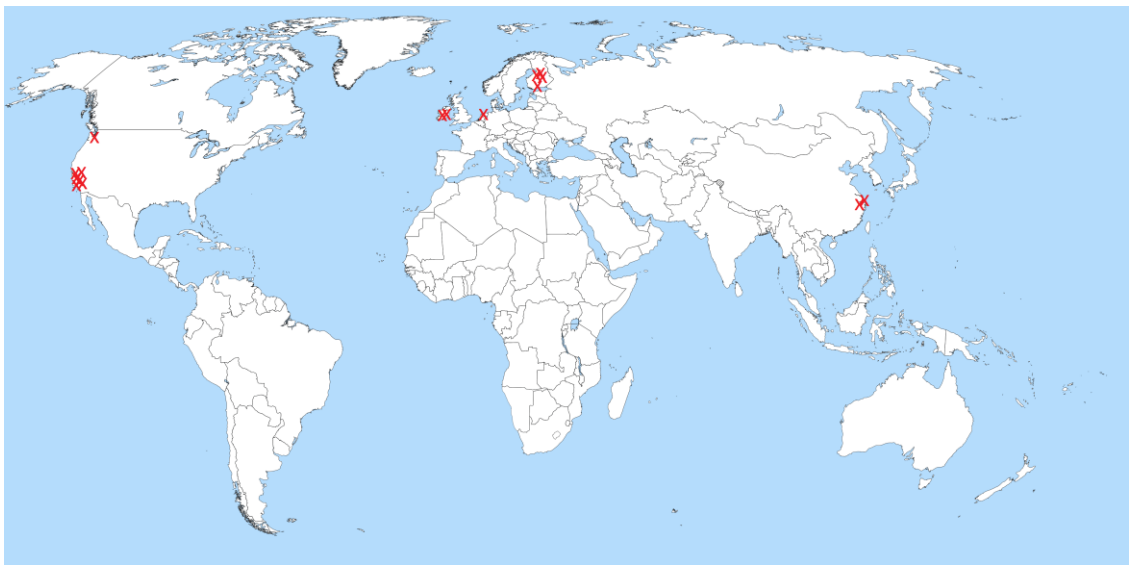
Htc:n havaittiin ottavan yhteyttä yhteensä kymmeneen eri IP-osoitteeseen. Tämä määrä on omiaan aiheuttamaan pohdintaa siitä, että ovatko nämä kaikki yhteydenotot käyttäjän kannalta aivan välttämättömiä. Todennäköisesti suurin osa yhteydenotoista on täysin harmittomia kuten esimerkiksi säätietojen hakeminen sääwidgetille, mahdollisesti automaattiset päivitystarkitukset sekä päivämäärä- ja aikatietojen lataaminen. Jäljelle jää kuitenkin useita kohteita ja dataa, joiden sisältöä voidaan vain arvuutella tai spekuloida kuten vaikka HTTP-pyynnön URI:n perusteella.

Laitteen toiminnan kannalta tuskin on välttämätöntä ladata .bin-tiedostoa Amazonin tai RX-Networksin palvelimelta. Useat yhteydenotot Googlen palvelimille ovat osittain ymmärrettävissä mahdollisilla käyttöjärjestelmän päivitystarkistuksilla tai muulla vastaavalla, mutta yhteydenottoja oli kuitenkin useita ja useille eri palvelimille ja se jättää spekulaatioille tilaa, että ovatko nämä aivan kaikki yhteydenotot täysin välttämättömiä vai sisältävätkö ne jotakin käyttäjän kannalta ei-haluttua. Jos mahdollisia käyttöjärjestelmäpäivityksiä tarkistetaan Googlen palvelimilta niin pohdittavaksi jää millä perusteella on ladattu HTTP:n avulla tiedosto Taiwan Fixed Network CO LTD:n palvelimelta. Googlen palvelimien kanssa avatuista TCP- tai TCP/SSL-istunnoista on mahdotonta sanoa, miksi ne kaikki tapahtuvat ja HTTP-pyyntöjen sisältämistä nimikentistä on myös hyvin vaikea päätellä yhteyksien tarkoitusta.

4.2 Huawei Mediapad 10 Link+

Laitteen tarkemmat tekniset tiedot saatiin laitteen IMEI-koodin perusteella **https://imeidata.net** –sivustolta. Alla olevat tiedot on kopioitu suoraan mainitulta sivuilta sellaisenaan.

IMEI:	864416020980598
Allocating	Body: TAF (China)
Type Allocation Code:	86441602
Serial Number:	098059
Luhn Checksum:	8
Manufacturer:	HUAWEI TECHNOLOGIES CO LTD
Brand:	HUAWEI
Model:	HUAWEI MEDIAPAD 10 LINK+
Band:	GPS, GSM 1800, GSM 1900, GSM 900, GSM850 (GSM800), LTE FDD BAND 1, LTE FDD BAND 20, LTE FDD BAND 3, LTE FDD BAND 7, LTE TDD BAND 38, LTE TDD BAND 40, WCDMA FDD Band I, WCDMA FDD Band II, WCDMA FDD Band V, WCDMA FDD Band VIII, WiFi.



KUVA 25. Kartta palvelimista joihin Huawei Mediapad -älylaite otti yhteyttä

Huawein havaittiin ottavan yhteyttä yhteensä neljääntoista eri IP-osoitteeseen. Tämä määrä on omiaan aiheuttamaan pohdintaa siitä, että ovatko nämä kaikki yhteydenotot käyttäjän kannalta aivan välttämättömiä. Todennäköisesti suurin osa yhteydenotoista on täysin harmittomia kuten esimerkiksi säätietojen hakeminen sääwidgetille, mahdolliset automaattiset päivitystarkitukset sekä päivämäärä- ja aikatietojen lataaminen. Jäljelle jää kuitenkin useita kohteita ja dataa, joiden sisältöä voidaan vain arvuutella tai spekuloida kuten vaikka HTTP-pyynnön URI:n perusteella.

Jonkin verran pohdiskeltavaa voidaan saada irti palvelimien nimistä tai pyyntöjen sisällöstä, kuten ”**www.googleadservices.com**” sekä HTTP-pyynnön sisällön sisältämä sanapari ”**remarketing_only**” tai **”/pagead/**”. Palvelimen nimi sekä pyynnön sisältö viittaavat siihen, että aivan kaikki yhteydenotot Googlen palvelimille eivät ole pelkästään täysin vilpittömästi hyvää tarkoittavia, vaan, että yhteydenotto liittyy tavalla tai toisella mainontaan tai markkinointiin. Eli se ei siis ole millään tavalla välttämätön toimenpide laitteen käyttäjän kannalta.

Amazonin palvelimelle tehty HTTP POST -pyynnön sisältämästä osuudesta ”**/hid_and_common/**” voisi tehdä sellaisen johtopäätöksen, että jotain tehdään ”hid” eli salassa. ”**GetCondition.action**” viittaa myös siihen, että jotakin tietoa halutaan käyttäjän laitteesta. Myös se, että HTTP POST -pyyntöön voidaan sisällyttää jotakin tietoja käyttäjältä on omiaan lisäämään epäilystä tämänkin yhteydenoton vilpittömyyteen.

China Telecomin palvelimelle tehty HTTP-pyyntö, joka sisältää mm. kyseisen laitteen IMEI-koodin herättää myöskin hyvin paljon epäilyksiä. Epäilyksiä ei myöskään vähennä se, että kyseinen yhteydenotto tapahtui heti sen jälkeen kun laitteen näyttö oli lukittu ja sammunut. Täyttä varmuutta asiasta ei voi vallitsevissa puitteissa saada, mutta pohdittavaksi jää kuinka vilpitön tämä yhteydenotto on.

5 YHTEENVETO

Työssä käytetty protokolla-analysaattori oli hieman jo vanhentunutta tekniikkaa, koska uudemmalla 4G-tekniikoita tukevalla analysaattorilla olisi voitu tutkia hieman uudempia älylaitteita. Vanhan analysaattorin kanssa ongelmia aiheutti myös se, että siinä käytetty USIM-kortti oli kooltaan mini-SIM. Sitä ei ollut vallitsevissa olosuhteissa mahdollista leikata eikä kopioida micro-SIM-kokoon. Tämä seikka rajoitti tutkittavien laitteiden määrää merkittävästi. Tarkoitus oli tutkia mahdollisiman monen eri älylaitteen toimintaa, mutta vallitsevissa olosuhteissa oli mahdollista saada ainoastaan kaksi tutkimukseen soveltuvaa älylaitetta.

Työssä saadut tulokset kuitenkin osoittavat, että molempien tutkittujen älylaitteiden tietoliikenteessä oli mahdollista epätoivottua liikennettä. Varsinkin uudemmassa älylaitteessa oli useita erikoisia ja mielenkiintoisia yhteydenottoja tietyille palvelimille, joka saattaa viitata siihen, että kaikkein uusimmissa laitteissa epätoivottua liikennettä olisi havaittu enemmän. Käytetyllä ns. ”nollabudjetin” laitteistollakin oli yllättävän hyvät puitteet tutkia työssä tavoiteltuja asioita.

Työssä tavoiteltu asioista oppiminen onnistui juuri siinä mittakaavassa kuin sen pitikin. Uutta asiaa tuli esille sopivissa määrin, sekä asioiden kohtuuton ns. ”rönsyäminen” oli mahdollista pitää kurissa. TCP/IP-protokollapinosta sekä varsinkin Wiresharkin käytöstä saatu oppi on arvokasta perustietoa tulevan osaamisen rakentamiselle. Työ oli miellyttävä tehdä, vaikkei uusimpia laitteita ollutkaan käytettävissä. Olisi mielenkiintoista rakentaa sellainen mittausympäristö, jonka avulla saisi tutkittua uusimpia mahdollisia älylaitteita ja päästä kiinni mitattuun dataan mahdollisimman syvälle. Sellaiselle systeemille olisi varmasti tulevaisuudessa kysyntää.

LÄHTEET

https://wiki.wireshark.org

http://www.imei.info

https://imeidata.net

Floyd Wilder, A guide to the TCP/IP protocol suite, 1998

https://en.wikipedia.org/wiki/File:A_large_blank_world_map_with_oceans_marked_in_blue.svg

https://ipinfo.io

http://www.ip-tracker.org

https://geoiptool.com

http://tools.tracemyip.org

LIITTEET

Liite 1. HTC Desire –älylaite kytkeytyneenä 3G-verkkoon 04.06.2015 1 (3)

1. 54.230.98.36
   Käytetyt protokollat TCP ja HTTP
   ISP: Amazon Technologies
   Organisaatio: Amazon.com
   Maa: Yhdysvallat
   Osavaltio/Maakunta: Washington
   Kaupunki: Seattle
   Aikavyöhyke: America/ Los Angeles
   Host: server-54-230-98-36.arn1.r.cloudfront.net
   DUT teki HTTP –pyynnön **xtra3.gpsonextra.net** –palvelimelle liittyen **xtra.bin** –tiedostoon, joka siirrettiin TCP-istunnolla. Tämä yhteydenotto tapahtui heti kun DUT oli käynnistynyt sekä kytkeytynyt 3G-verkkoon.

2. 216.58.209.142
   Käytetyt protokollat TCP ja SSL
   ISP: Google
   Organisaatio: Google inc.
   Maa: Yhdysvallat
   Osavaltio/Maakunta: Kalifornia
   Kaupunki: Mountain View
   Host: arn09s05-in-f142.1e100.net
   DUT aloitti kyseisen hostin kanssa TCP/SSL-istunnon, jonka aikana siirtyi parikymmentä TCP-pakettia. Tämä yhteydenotto tapahtui heti kun DUT oli käynnistynyt sekä kytkeytynyt 3G-verkkoon.

3. 131.107.13.100 2 (3)

   Käytetyt protokollat TCP/Daytime

   ISP: Microsoft corp.

   Organisaatio: Microsoft corp.

   Maa: Yhdysvallat

   Osavaltio/Maakunta: Washington

   Kaupunki: Bellevue

   Host: 131.107.13.100

   DUT aloitti Daytime-protokollaan liittyen puolenkymmentä lyhyttä muutaman paketin pituista TCP-istuntoa. Tämä yhteydenotto tapahtui heti kun DUT oli käynnistynyt sekä kytkeytynyt 3G-verkkoon.

4. 62.183.170.17

   Käytetyt protokollat TCP ja HTTP

   ISP: DNA Oy

   Organisaatio: Superlon Oy

   Maa: Suomi

   Osavaltio/Maakunta: Uusimaa

   Kaupunki: Vantaa

   Host: 62-183-170-17.co.dnainternet.fi

   DUT teki HTTP-pyynnön **htc.accuweather.com** –palvelimelle liittyen **/widget/htc/lat-lon-search.asp?ac=TR2cra9U&lat=28.622436&lon=77.310609&nocache=1433418426776** –tiedostoon, joka siirrettiin TCP-istunnolla. TCP-istunnon pituus oli kymmenkunta pakettia. Tämä yhteydenotto tapahtui kun DUT:n näyttö avattiin kun se oli ensin ollut lukittuneena ja sammuneena.

5. 216.58.209.132 3 (3)

   Käytetyt protokollat TCP/SSL

   ISP: Google

   Organisaatio: Google inc.

   Maa: Yhdysvallat

   Osavaltio/Maakunta: Kalifornia

   Kaupunki: Mountain View

   Aikavyöhyke: America/ Los Angeles

   Host: arn09s05-in-f4.1e100.net

   DUT aloitti kyseisen hostin kanssa TCP/SSL-istunnon, jonka aikana siirtyi kymmenkunta TCP-pakettia. Tämä yhteydenotto tapahtui heti kun DUT oli käynnistynyt sekä kytkeytynyt 3G-verkkoon.

Liite 2. HTC Desire –älylaite kytkeytyneenä WLAN-verkkoon 06.07.2015 1 (6)

1. 72.51.26.219

   Käytetyt protokollat TCP ja HTTP

   ISP: PEER 1 Network

   Organisaatio: RX Networks

   Maa: Kanada / Yhdysvallat

   Osavaltio/Maakunta: Brittiläinen Kolumbia / New York

   Kaupunki: Vancouver / New York

   Aikavyöhyke: America / New York

   Host: 72.51.26.219

   DUT teki HTTP-pyynnön **xtra1.gpsonextra.net** –palvelimelle liittyen **xtra.bin** –tiedostoon, joka siirrettiin TCP-istunnolla. Tämä yhteydenotto tapahtui heti kun DUT oli käynnistynyt sekä kytkeytynyt WLAN-verkkoon.

2. 62.183.170.17

   Käytetyt protokollat TCP ja HTTP

   ISP: DNA Oy

   Organisaatio: Superlon Oy

   Maa: Suomi

   Osavaltio/Maakunta: Uusimaa

   Kaupunki: Vantaa

   Aikavyöhyke: Europe / Helsinki

   Host: 62-183-170-17.co.dnainternet.fi

   DUT teki useita HTTP-pyyntöjä **htc.accuweather.com** –palvelimelle liittyen, jotka siirrettiin TCP-istunnoilla. Tämä yhteydenotto tapahtui heti kun DUT oli käynnistynyt sekä kytkeytynyt WLAN-verkkoon. Kaikkiaan noin viisikymmentä TCP-pakettia siirtyi.

Pyyntöjä oli useampi kappale, joten ne on listattu tässä allekkain: 2 (6)

-/widget/htc/forecast-da-ta_v3.asp?ac=TR2cra9U&loccode=NAM%7CUS%7CNY%7CNEW+YORK&nocache=315964963197

-/widget/htc/forecast-da-ta_v3.asp?ac=TR2cra9U&loccode=EUR%7CPL%7CPL007%7CWARSZAWA&nocache=315964963574

-/widget/htc/forecast-da-ta_v3.asp?ac=TR2cra9U&loccode=EUR%7CIT%7CIT007%7CROMA&nocache=315964963784

-/widget/htc/forecast-da-ta_v3.asp?ac=TR2cra9U&loccode=EUR%7CES%7CSP008%7CBARCELONA&nocache=315964963919

-/widget/htc/forecast-da-ta_v3.asp?ac=TR2cra9U&loccode=EUR%7CFR%7CFR012%7CPARIS&nocache=315964964036

-/widget/htc/forecast-da-ta_v3.asp?ac=TR2cra9U&loccode=EUR%7CUK%7CUK124%7CLONDON&nocache=315964964411

-/widget/htc/lat-lon-search.asp?ac=TR2cra9U&lat=61.501867&lon=23.802641&nocache=315964964627

-/widget/htc/forecast-da-ta_v3.asp?ac=TR2cra9U&loccode=NAM%7CUS%7CNY%7CNEW+YORK&nocache=315964965090

-/widget/htc/forecast-da-ta_v3.asp?ac=TR2cra9U&loccode=EUR%7CPL%7CPL007%7CWARSZAWA&nocache=315964965502

-/widget/htc/forecast-da-ta_v3.asp?ac=TR2cra9U&loccode=EUR%7CIT%7CIT007%7CROMA&nocache=315964965684

-/widget/htc/forecast-da-ta_v3.asp?ac=TR2cra9U&loccode=EUR%7CES%7CSP008%7CBARCELONA&nocache=315964965909

-/widget/htc/forecast-da-ta_v3.asp?ac=TR2cra9U&loccode=EUR%7CFR%7CFR012%7CPARIS&nocache=315964966590

-/widget/htc/forecast-da-ta_v3.asp?ac=TR2cra9U&loccode=EUR%7CUK%7CUK124%7CLONDON&nocache=315964966737

-/widget/htc/lat-lon-search.asp?ac=TR2cra9U&lat=61.501867&lon=23.802641&nocache=315964967078

-/widget/htc/lat-lon-search.asp?ac=TR2cra9U&lat=61.502699&lon=23.807248&nocache=315964981859

-/widget/htc/lat-lon-search.asp?ac=TR2cra9U&lat=61.501909&lon=23.801273&nocache=1436159499676

3. 60.199.250.34
   Käytetyt protokollat TCP ja HTTP
   ISP: Taiwan Fixed Network CO LTD
   Organisaatio: Taiwan Fixed Network CO LTD
   Maa: Taiwan
   Osavaltio/Maakunta: Tai-Pei
   Kaupunki: Taipei
   Aikavyöhyke:
   Host: 60-199-250-34.static.tfn.net.tw
   DUT teki kaksi HTTP-pyyntöä **andchin.htc.com** –palvelimelle liittyen **/android/checkin** –tiedostoon, jotka siirrettiin TCP -stunnolla. Tämä yhteydenotto tapahtui heti kun DUT oli käynnistynyt sekä kytkeytynyt WLAN-verkkoon.

4. 131.107.13.100
   Käytetyt protokollat TCP ja Daytime
   ISP: Microsoft Corp.
   Organisaatio: Microsoft Corp.
   Maa: Yhdysvallat
   Osavaltio/Maakunta: Washington
   Kaupunki: Bellevue
   Aikavyöhyke:
   Host: 131.107.13.100
   DUT aloitti Daytime-protokollaan liittyen kaksi lyhyttä noin kymmenen paketin pituista TCP-istuntoa. Tämä yhteydenotto tapahtui heti kun DUT oli käynnistynyt sekä kytkeytynyt WLAN-verkkoon.
5. 62.44.200.171

Käytetyt protokollat TCP ja HTTP

ISP: DNA Oy

Organisaatio: TietoEnator

Maa: Suomi

Osavaltio/Maakunta: Etelä-Suomi

Kaupunki: Lahti

Aikavyöhyke: Europe / Helsinki

Host: 62-44-200-171.co.dnainternet.fi

DUT teki kaksi HTTP-pyyntöä **fotadl.htc.com** –palvelimelle liittyen **/OTA_Bravo_Froyo_HTC_WWE_2.29.405.52.29.405.2_releasedauhl6jhok5cmdm6.zip** –tiedostoon joka siirrettiin TCP-istunnolla, jossa paketteja siirtyi noin sata. Tämä yhteydenotto tapahtui heti kun DUT oli käynnistynyt sekä kytkeytynyt WLAN-verkkoon.

6. 216.58.209.100

Käytetyt protokollat TCP ja SSL

ISP: Google inc.

Organisaatio: Google

Maa: Yhdysvallat

Osavaltio/Maakunta: Kalifornia

Kaupunki: Mountain View

Aikavyöhyke: America / Los Angeles

Host: arn06s07-in-f100.1e100.net

DUT aloitti kyseisen hostin kanssa TCP/SSL-istunnon, jonka aikana siirtyi noin sata TCP-pakettia. Tämä yhteydenotto tapahtui heti kun DUT oli käynnistynyt sekä kytkeytynyt WLAN-verkkoon.

7. 216.58.209.110 6 (6)

Käytetyt protokollat TCP, SSL ja HTTP

ISP: Google inc.

Organisaatio: Google

Maa: Yhdysvallat

Osavaltio/Maakunta: Kalifornia

Kaupunki: Mountain View

Aikavyöhyke: America / Los Angeles

Host: arn06s07-in-f14.1e100.net

DUT teki HTTP-pyynnön **android.clients.google.com** –palvelimelle liittyen **/checkin** –tiedostoon, joka siirrettiin TCP/SSL-istunnolla. Tämä yhteydenotto tapahtui heti kun DUT oli käynnistynyt sekä kytkeytynyt WLAN-verkkoon.

1. 64.233.161.188
   Käytetyt protokollat TCP
   ISP: Google
   Organisaatio: Google
   Maa: Yhdysvallat
   Osavaltio/Maakunta: Kalifornia
   Kaupunki: Mountain View
   Aikavyöhyke: America/ Los Angeles
   Host: lh-in-f188.1e100.net
   DUT kävi TCP-pakettien vaihtoa hetkittäin koko noin kolmen tunnin mittaus-jakson ajan. Tiedonsiirto käsitti joitakin kymmeniä TCP-paketteja.

2. 62.44.200.177
   Käytetyt protokollat TCP ja HTTP
   ISP: DNA Oy
   Organisaatio:
   Maa: Suomi
   Osavaltio/Maakunta: Uusimaa
   Kaupunki: Helsinki
   Host: 62-44-200-177.co.dnainternet.fi
   DUT teki HTTP-pyynnön **gllto2.glpals.com** –palvelimelle liittyen **/7day/v3/latest/lto2.dat** –tiedostoon, joka siirrettiin TCP-istunnolla. TCP-istunnon pituus oli noin sata TCP -pakettia. Tämä yhteydenotto tapahtui heti kun DUT oli käynnistynyt sekä kytkeytynyt 3G-verkkoon.

3. 62.78.98.182 2 (5)

   Käytetyt protokollat TCP ja SSL

   ISP: DNA Oy

   Organisaatio:

   Maa: Suomi

   Osavaltio/Maakunta: Kainuu

   Kaupunki:

   Aikavyöhyke: Europe / Helsinki

   Host:

   DUT aloitti kyseisen hostin kanssa TCP/SSL-istunnon, jonka aikana siirtyi noin kaksikymmentä TCP-pakettia. Tämä yhteydenotto tapahtui heti kun DUT oli käynnistynyt sekä kytkeytynyt 3G-verkkoon.

4. 216.58.209.98

   Käytetyt protokollat TCP ja HTTP

   ISP: Google

   Organisaatio: Google

   Maa: Yhdysvallat

   Osavaltio/Maakunta: Kalifornia

   Kaupunki: Mountain View

   Host: arn06s07-in-f2.1e100.net

   DUT teki HTTP-pyynnön **www.googleadservices.com** –palvelimelle liittyen **/pagead/conversion/1001680686/?label=4dahCKKczAYQrt7R3QM&value=&muid=N42o-pfz2PAlQ9H4THK4xw&bundleid=com.google.android.youtube&appversion=5.9.0.13&osversion=4.4.2&sdkversion=ct-sdk-a-v1.1.0&remarketing_only=1&timestamp=1435048876&data=screen_name%3D%3CAndroid_YT_Open_App%3E**

   –tiedostoon, joka siirrettiin TCP-istunnolla. TCP-istunnon pituus oli kymmenkunta pakettia. Tämä yhteydenotto tapahtui heti kun DUT oli käynnistynyt sekä kytkeytynyt 3G-verkkoon.

5. 62.78.98.183 3 (5)

   Käytetyt protokollat TCP ja SSL

   ISP: DNA Oy

   Organisaatio:

   Maa: Suomi

   Osavaltio/Maakunta: Kainuu

   Kaupunki:

   Aikavyöhyke: Europe / Helsinki

   Host:

   DUT aloitti kyseisen hostin kanssa TCP/SSL-istunnon, jonka aikana siirtyi noin viisi tuhatta TCP-pakettia. Tämä yhteydenotto tapahtui heti kun DUT oli käynnistynyt sekä kytkeytynyt 3G-verkkoon.

6. 104.76.53.168

   Käytetyt protokollat TCP ja HTTP

   ISP: Akamai Technologies

   Organisaatio: Akamai International, BV

   Maa: Hollanti

   Osavaltio/Maakunta: Pohjois-Hollanti

   Kaupunki: Amsterdam

   Aikavyöhyke: Europe / Amsterdam

   Host: a104-76-53-168.deploy.static.akamaitechnologies.com

   DUT teki HTTP-pyynnön **huawei2.accu-weather.com** –palvelimelle liittyen **/widget/huawei2/weather-data.asp?location=cityId%3A133091** –tiedostoon, joka siirrettiin TCP-istunnolla. TCP-istunnon pituus oli kymmenkunta pakettia. Tämä yhteydenotto tapahtui heti kun DUT oli käynnistynyt sekä kytkeytynyt 3G-verkkoon.

7. 54.194.186.54 4 (5)

   Käytetyt protokollat TCP ja HTTP

   ISP: Amazon Technologies Inc.

   Organisaatio: Amazon.com, Inc.

   Maa: Irlanti

   Osavaltio/Maakunta: Dublin

   Kaupunki: Dublin

   Aikavyöhyke: Europe / Dublin

   Host: ec2-54-194-186-54.eu-west-1.compute.amazonaws.com

   DUT teki HTTP post –pyynnön **query.hicloud.com:80** –palvelimelle liittyen **/hid_and_common/v2/Check.action?latest=true** –tiedostoon, joka siirrettiin TCP-istunnolla. TCP-istunnon pituus oli kymmeniä paketteja. Tämä yhteydenotto tapahtui heti kun DUT oli käynnistynyt sekä kytkeytynyt 3G-verkkoon.

8. 216.58.209.110

   Käytetyt protokollat TCP

   ISP: Google

   Organisaatio: Google

   Maa: Yhdysvallat

   Osavaltio/Maakunta: Kalifornia

   Kaupunki: Mountain View

   Aikavyöhyke: America / Los Angeles

   Host: arn06s07-in-f110.1e100.net

   DUT suoritti jonkinlaista TCP-istuntoa kyseisen hostin kanssa. Istunto sisälsi sekalaisesti muutamia FIN-, ACK- ja RST –viestejä. Tämä yhteydenotto tapahtui heti kun DUT oli käynnistynyt sekä kytkeytynyt 3G-verkkoon.

9. 115.239.211.92 5 (5)

Käytetyt protokollat TCP ja HTTP

ISP: China Telecom Zhejiang

Organisaatio: China Telecom Hangzhou

Maa: Kiina

Osavaltio/Maakunta: Zhejiang

Kaupunki: Hangzhou

Aikavyöhyke: Asia / Chongqing

Host: 115.239.211.92

DUT teki HTTP-pyynnön **nsclick.baidu.com** –palvelimelle liittyen **/v.gif?pid=121&type=7&mc=&null&mod=android&uid=[IMEI]864416020980598&dm=MediaPad%2010%20Link+&ns=1&action=start&sv=4.4.2&carrier=&ns=1&mc=&fl=0**

–tiedostoon, joka siirrettiin TCP-istunnolla. TCP-istunnon pituus oli kymmenkunta pakettia. Tämä yhteydenotto tapahtui heti sen jälkeen kun DUT:n näyttö oli lukittu ja pimeänä.

Liite 4. Huawei Medipad -älylaite kytkeytyneenä WLAN-verkkoon 24.06.2015 1 (4)

1. 62.78.98.178

   Käytetyt protokollat TCP ja HTTP

   ISP: DNA Oy

   Organisaatio: DNA Oy

   Maa: Suomi

   Osavaltio/Maakunta: Kainuu

   Kaupunki:

   Aikavyöhyke: Europe / Helsinki

   Host:

   DUT teki HTTP-pyynnön **62.78.98.178** –palvelimelle liittyen **/generate_204** –tiedostoon, joka siirrettiin TCP-istunnolla. TCP-istunnon pituus oli kymmenkunta pakettia. Tämä yhteydenotto tapahtui heti kun DUT oli käynnistynyt sekä kytkeytynyt WLAN-verkkoon.

2. 115.239.211.92

   Käytetyt protokollat TCP ja HTTP

   ISP: China Telecom Zhejiang

   Organisaatio: China Telecom Hangzhou

   Maa: Kiina

   Osavaltio/Maakunta: Zhejiang

   Kaupunki: Hangzhou

   Aikavyöhyke:

   Host:

   DUT teki kaksi kertaa HTTP-pyynnön **nsclick.baidu.com** –palvelimelle liittyen **/v.gif?pid=121&type=7&mc=&null&mod=android&uid=[IMEI]NULL&dm=MediaPad%2010%20Link+&ns=2&action=start&sv=4.4.2&carrier=&ns=2&mc=&fl=0**

   –tiedostoon, joka siirrettiin TCP-istunnolla. TCP-istunnon pituus oli kymmenkunta pakettia. Ensimmäinen yhteydenotto tapahtui heti kun DUT oli käynnistynyt sekä kytkeytynyt WLAN-verkkoon ja toinen myöhemmin heti kun DUT:n näyttö oli lukittunut ja pimentynyt.

3. 54.192.99.135

Käytetyt protokollat TCP ja HTTP

ISP: Amazon Technologies

Organisaatio: Amazon.com

Maa: Yhdysvallat

Osavaltio/Maakunta: Washington

Kaupunki: Seattle

Aikavyöhyke:

Host: server-54-192-99-135.arn1.r.cloudfront.net

DUT teki HTTP-pyynnön **gllto1.glpals.com** –palvelimelle liittyen **/7day/v3/latest/lto2.dat** –tiedostoon, joka siirrettiin TCP-istunnolla. TCP-istunnon pituus oli kymmenkunta pakettia. Yhteydenotto tapahtui heti kun DUT oli käynnistynyt sekä kytkeytynyt WLAN-verkkoon.

4. 64.233.164.188

   Käytetyt protokollat TCP

   ISP: Google

   Organisaatio: Google

   Maa: Yhdysvallat

   Osavaltio/Maakunta: Kalifornia

   Kaupunki: Mountain View

   Host: lf-in-f188.1e100.net

   DUT aloitti kyseisen hostin kanssa TCP-istunnon, jonka aikana siirtyi noin sata TCP-pakettia. Tämä yhteydenotto alkoi heti DUT oli käynnistynyt sekä kytkeytynyt WLAN-verkkoon ja se kesti lähes koko otannan ajan.

5. 216.58.209.98 3 (4)

   Käytetyt protokollat TCP ja HTTP

   ISP: Google

   Organisaatio: Google

   Maa: Yhdysvallat

   Osavaltio/Maakunta: Kalifornia

   Kaupunki: Mountain View

   Aikavyöhyke:

   Host: arn06s07-in-f98.1e100.net

   DUT teki HTTP-pyynnön **www.googleadservices.com** –palvelimelle liittyen **/pagead/conversion/1001680686/?label=4dahCKKczAYQrt7R3QM&value=&muid=N42o-pfz2PAlQ9H4THK4xw&bundleid=com.google.android.youtube&appversion=5.9.0.13&osversion=4.4.2&sdkversion=ct-sdk-a-v1.1.0&remarketing_only=1&timestamp=1435124601&data=screen_name%3D%3CAndroid_YT_Open_App%3E**

   –tiedostoon, joka siirrettiin TCP-istunnolla. TCP-istunnon pituus oli kymmenkunta pakettia. Yhteydenotto tapahtui heti kun DUT oli käynnistynyt sekä kytkeytynyt WLAN-verkkoon.

6. 54.72.215.57

   Käytetyt protokollat TCP ja HTTP

   ISP: Amazon Technologies

   Organisaatio: Merck and Co.

   Maa: Irlanti

   Osavaltio/Maakunta: Dublin

   Kaupunki: Dublin

   Aikavyöhyke: Europe / Dublin

   Host: ec2-54-72-215-57.eu-west-1.compute.amazonaws.com

   DUT teki kaksi HTTP-pyyntöä **query.hicloud.com:80** –palvelimelle liittyen **/hid_and_common/v2/Check.action?latest=true** –tiedostoon sekä **/hid_and_app_common/v2/GetCondition.action** -tiedostoon, jotka siirrettiin TCP-istunnoilla. Kunkin TCP-istunnon pituus oli kymmenkunta pakettia. Tämä yhteydenotto tapahtui heti kun DUT oli käynnistynyt sekä kytkeytynyt WLAN-verkkoon.

7. 173.194.71.188 4 (4)

Käytetyt protokollat TCP

ISP: Google

Organisaatio: Google

Maa: Yhdysvallat

Osavaltio/Maakunta: Kalifornia

Kaupunki: Mountain View

Aikavyöhyke:

Host: lb-in-f188.1e100.net

DUT aloitti kyseisen hostin kanssa TCP-istunnon, jonka aikana siirtyi kymmeniä TCP-paketteja. Tämä yhteydenotto tapahtui heti kun DUT oli käynnistynyt sekä kytkeytynyt WLAN-verkkoon.