Aalto University
School of Science
Bachelor's Programme in Science and Technology

DNS Enumeration Techniques (Working title)

Bachelor's Thesis

xx. xxxxxkuuta 20xx

Tuomas Välimäki

Aalto-yliopisto
Perustieteiden korkeakoulu
Teknistieteellinen kandidaattiohjelma

KANDIDAATINTYÖN
TIIVISTELMÄ

Tekijä:	Tuomas Välimäki
Työn nimi:	DNS Enumeration Techniques
Päiväys:	xx. xxxxxkuuta 20xx
Sivumäärä:	Kirjoita tähän oikea määrä, tässä esimerkissä 23
Pääaine:	Tietotekniikka
Koodi:	SCI3027
Vastuuopettaja:	Professori Tuomas Aura
Työn ohjaaja(t):	Titteli Jacopo Bufalino (Tietojenkäsittelytieteen laitos)
Delorem ipsum	
Avainsanat:	avain, sanoja, niitäkin, tähän, vielä, useampi, vaikkei, niitä, niin, montaa, oikeasti, tarvitse
Kieli:	Suomi

Aalto University
School of Science
Bachelor's Programme in Science and Technology

ABSTRACT OF
BACHELOR'S THESIS

Author:	Tuomas Välimäki
Title of thesis:	DNS Enumeration Techniques
Date:	MonthName 31, 20xx
Pages:	Kirjoita tähän oikea määrä, tässä esimerkissä 23
Major:	Tietotekniikka
Code:	SCI3027
Supervisor:	Tuomas Aura, Professor
Instructor:	Jacopo Bufalino, titleOfInstructor (Department of Information and Computer Science)
Ja sama englanniksi.	
Keywords:	key, words, the same as in FIN/SWE
Language:	English

Contents

1 Introduction

The first stage of committing a cyber attack or a penetration test is reconnaissance or footprinting to acquire information about networking infrastructure of the target. Various footprinting techniques may be used to query open sources, such as using advanced search features of search engines and WHOIS queries. One such technique is Domain Name System (DNS) enumeration which uses public DNS records to gather information about the target without actually probing the target network. The Domain Name System may reveal information such as IP addresses, domains, subdomains, mail exchange services and other information.

Method of this study is mainly to conduct a literary research about the existing DNS enumeration techniques and their operating principles, not on particular tools. The motivation is that there is no shortage of blog postings explaining the use tools with little or no emphasis on the underlying principles.

The goals of this study is as follows:

- Conduct a literary study about existing DNS enumeration techniques
- As services move to the cloud investige how DNS enumeration techniques can be leveraged to gather information about cloud services.
- Present some use cases

DNS has been and still is vulnerable to attacks such as DNS cache poisoning but discussing these kinds of attacks in detail is out of the scope of this study.

2 The Domain Name System

The Domain Name system or DNS is a fundamental part of the Internet infrastructure. This chapter gives a brief overview of DNS, related security issues and recent developments related to this study.

2.1 Overview

Domain Name System [1034, 1035] is a distributed database implemented in a hierarchy of DNS servers with delegated authority that stores information about services and other resources in the Internet. Notably, DNS stores information that maps host names to IP addresses. The DNS specifies the functionality of DNS servers and the DNS protocol which on the most part is based on the UDP protocol. DNS is part of the Internet Protocol

Suite. DNS is an application layer protocol commonly employed by other application layer protocols such as HTTP or FTP. [7][15]

When a client makes a query e.g to retrieve an IP address for a host name, the corresponding IP address is resolved in a recursive manner by a DNS resolver. At the top level there are 13 logical root name servers distributed across the globe named from A to M. Unless the result is not found in cache the root name server is queried first which delegates the query for a top level domain such as .com., to a Top Level Server Domain server or TLD server. The iteration continues until an Authoritative Name Server is found for the host. The query result is returned to the client via DNS resolver. See Figure1 for illustration of the process. [7][15]

In addition there is another class of DNS servers called the local DNS Server which is stricly not part of the DNS hierarcy, but is part of the DNS infratructure. [7]

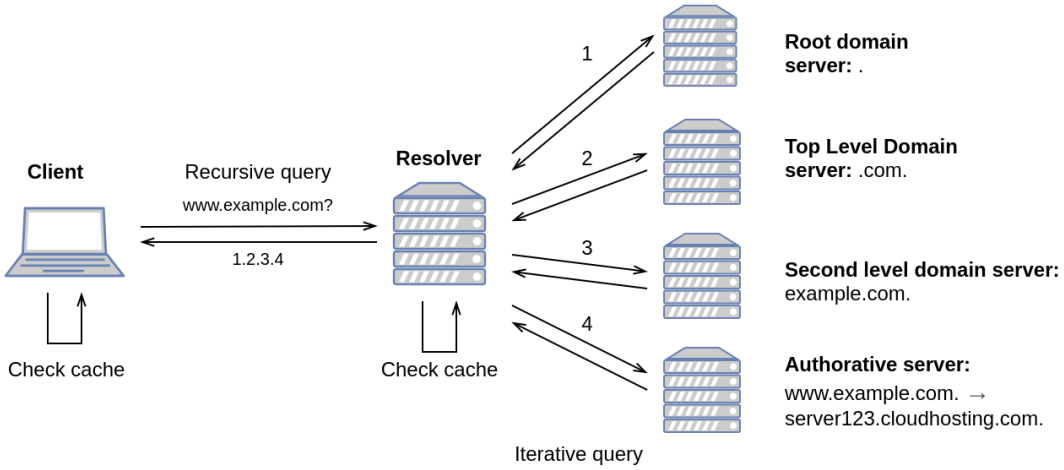

Figure 1: A simplistic presentation of resolving an IP address for a host `www.example.com`. In this example Authoritative name server does not have a record for the IP address. Instead, Authoritative name server has a CNAME record (see Table 1). Hostname `www.example.com` is an "alias" that points to a Canonical Name, `server123.cloudhosting.com`. This triggers a new iterative query until IP address is resolved.

2.2 DNS Record Types

A DNS database or a DNS record has multiple record types. Most common and relevant for this study are listed in Figure 1. Among A and AAAA records, PTR record has a special interest related to this study since it allows reverse DNS lookup which maps an IP address to a hostname.

Table 1: Most common DNS Record types.

Record Type	Description
A	IPv4 address for a host. [9]
AAAA	IPv6 address for a host RFC3596
MX	Mail exchange server. [9] ja 7505
CNAME	Canonical Name. Maps an ”alias” to a canonical name. [9]
SOA	Start Of Authority
PTR	A Pointer Record. Maps an IP addres to a hostname. [9]

2.3 DNS Zones

A DNS zone is a distinct part of domain namespace which is delegated to an entity such as an organization. An area of one or more subdomains that has been delegated for management and authority is called a DNS zone. DNS zones should not be associated with domain namespaces. A single DNS server may be responsible for multiple zones, and for replication, load distribution and security (e.g to deflect DDoS attacks[]) there are usually multiple domain name servers for each zone.[15]

In the example presented if Fig. 1 second level domain name server for `example.com` has delegated the responsibility of subdomain `www.example.com` for another zone.

If there are multiple domain name servers for a zone there is a primary DNS server which is replicated by secondary servers. A secondary DNS server maintains a read-only copy of the DNS zone file maintained in the primary DNS server. If modifications are made they are made into the DNS zone file of the primary DNS server. The process of secondary DNS server requesting an update and receiving this information is called a Zone Transfer. [15]

2.4 Publicity and Security of DNS

The instrinsic property of DNS records is that on the most part they are public by design and normal DNS queries are not encrypted. DNS system has a long history of being vulnerable for DNS spoofing and DNS cache poisoning where the attacker tricks DNS server to store false information in a DNS cache [15] [RFS3833].

DNS Security Extension or DNSSEC (defined originally in now obsolete [rfc 2065]) has been developed to provide end-to-end data integrity and source authenticity check

between the source of DNS data and the client. To achieve this DNSSEC uses public/private key pair signatures. Threaths of data disclosure were ruled out of scope of DNSSEC [RFS3833]. Although DNSSEC was standardized already in 1997 it is still not widely used but the adoption is progressing slowly [12]. DNSSEC relies on authentication chain. All root level domain name servers use DNSSEC signatures but if a TLD does not implement DNSSEC there can not be DNSSEC for any domain under such TLD [citation needed].

Transmission signatures or TSIG [RFC2845] use shared private keys to provide authentication of servers to secure actions such as zone transfers and dynamic updates of resource records.

In recent years new standards for encrypting DNS query traffic has been developed such as DNS over TCP (DoT) [RFC 7858], DNS Queries over HTTP (DoH) [RFC 8484] and DNS over DTLS [RFC 8094] to prevent passive information gathering.

* BIND? * DANE? * Dynamic Updating? * Zone poisoning? * SIG(0) ?

2.5 Recent development in DNS

* Using DNS to store all sorts of data, explosion of number of RR types, TXT RR ?

* Changes/advances/new fashions DNS infrastructure ??

3 DNS Enumeration

Due to the original design philosophy and easy access principle, DNS is vulnerable to information leakage and attacks such as DNS spoofing. Since DNS records on the most part are intended to be public DNS queries allow attackers the gather information about the target. DNS Enumeration is part of the reconnaissance stage where an attacker gathers information about targets network footprint. This includes gathering information about IP addresses, domains and subdomains. DNS Enumeration is considered to be part of the Open Source Intelligent or OSINT methodology where publicly available (”open source”) sources are used in an intelligence context [1]. DNS enumeration is commonly used jointly with other OSINT methods such as `whois` queries and exploiting advanced search engine features such as ”Google Dorks” [1].

This chapter will review the most common methods of DNS enumeration.

3.1 Basic DNS lookup

Every resource record or RR can be considered a five-tuple (Name, Type, Class, Time to Live, Value) [1035]. Some of the Types were listed in Table 1. In addition to Types (TYPE), DNS defines query types (QTYPE) which is a superset of types. The DNS protocol also defines a query class (QCLASS) as a superset of class (CLASS). Every query contains QNAME (fully qualifed domain name or FQDN), QTYPE and QCLASS [1035].

`Nslookup` and 'Domain Internet Grober' (`dig`) are common tools found in most Unix enviroments to carry out basic DNS queries. For example `dig -q www.example.com -t AAAA -c IN` returns an IPv6 address for `www.example.com` with query class `IN` (Internet). In practise the query class is now redundant since the query class `IN` is the only one in use but is required by the protocol definition.

Above example which returns an IP address for a host name is called a forward lookup. A reverse lookup is a query returning a host name for an IP address (PTR record).

3.2 Zone Transfer Attack

As explained in Section 2.3 each DNS zone has a primary server and secondary servers maintain read-only copies of primary servers zone file. DNS protocol defines a special type of query, Asynchronous Transfer Full Range or AXFR which requests for a transfer of an entire list of resource records for zone [RFC 1035] or a zone file. The DNS zone information may include sensitive information e.g about the internal infrastructure of a network of an organization. Although succeeding in unauthorized zone transfer requests is considered by some as a thing for the past [1] on a global-scale vulnerability assessment Skwarek et al. [13] were able to carry out approximately 11 million zone transfers containing information such as HINFO (information about OS and CPU etc.) records, and domains with `test.` and `dev.` prefixes etc.

The AXFR offers no authentication method [RFC 1035, 5936]. In order to prevent the vulneralibility from occurring the DNS server should be configured to only allow AXFR requests from trusted IP addresses. Additionally the use of TSIG provides authentication of trusted servers. Since AXFR uses TCP [RFC5936] using a firewall to block TCP traffic to port 56 is an option but would violate DNS specifications (DNS queries over X bytes should be transferred over TCP) [Hacking exposed].

3.3 Zone Enumeration

"Another vulnerability related to our work is so-called zone enumeration. Initially, ability to enumerate all the names in a zone was not considered as an error [2], however, later on, a compromise has been reached [22] that in certain cases, the knowledge of all the domain names in a zone can lead to security risks. RFC 5155 [22] provides some examples showing that due to this vulnerability, it is easier for an attacker to obtain email addresses for future spam campaigns or data useful during a reconnaissance phase of a network attack." Skwarek et al. [13]

3.4 Reverse DNS sweeping

"After building a list of IP network blocks used or reserved by the target organization, reverse DNS sweeping can gather details of hosts that may be protected or filtered but still have DNS hostnames assigned to them." [1]

What the hell is protected or filtered hosts?

3.5 Zone Enumeration

As explained in section 2.4 the purpose of DNSSEC is to provide end-to-end data integrity and source authenticity check in the Domain Name System. This section will not cover DNSSEC in detail but an important part of DNSSEC which is called an authenticated denial of of existence in DNS. The section will further discuss how the authenticated denial of existence can be leveraged to execute a DNS enumeration technique called Zone Walking or Zone Enumeration.

3.5.1 Denial of Existence in DNS

DNSSEC signatures are used only for signing the Resource Records in the DNS response message or packet. The DNS message header is not signed.

The DNS response message header contains a status code. If a DNS query is made for an existing name (QNAME), status code of the response header is NOERROR and the answer section contains Resource Records for the name in question, which are signed if DNSSEC is supported.

There are two cases of status codes corresponding to situations where requested Resource record does not exits.

- If a query is made for a name that does not exist the status code of the response is `NXDOMAIN` (Non-Existing Domain).

- If a query is made for a name that does exist but the requested resource record does not exist the status code of the response is `NOERROR`. Based on the response the resolver can infer that the type of response is of type called `NODATA`.

Since DNSSEC signature is not used to sign DNS message header the NXDOMAIN status cannot be trusted. In addition the DNSSEC signatures are precomputed. The original design of DNSSEC excluded online signing due to security reasons (to keep the private key offline) and the computational overhead. Therefore, offline signing the header is not feasible since it would require precomputing signatures for all conceivable nonexisting answers.

Above elaborates the issue with DNSSEC and authenticated denial of existence: if an empty answer is returned there are no resource records to sign. The first attempt to specify authenticated denial of existence was NXT resource record (defined in [RFC2535]) but this was superceded by NSEC resource record.

NSEC resource record indirectly lets the resolver to know that the name does not exist in the zone. Zone is sorted into canonical order [RFC 4034] and NSEC describes an interval between names. For example if a zone contains a domain names `a.domain.org` and `c.domain.org` and in canonical ordering there are no domain names in between in the zone, DNS query for a domain name `b.domain.org` returns (class and time to live omitted for simplicity):

```
Name              Type    Value
a.domain.org      NSEC    c.domain.org NS SOA TXT RRSIG NSEC DNSKEY
```

The answer above is returned since `b.domain.org` resides in the interval between `a.domain.org` and `c.domain.org`. The value returned contains the endpoint of the interval and a list of resource records types where RRSIG, NSEC and DNSKEY are related to DNSSEC.

NSEC records are also used in `NODATA` responses as is explained in [7129].

Aika lailla koko paska [rfc7129]

3.5.2 Zone Walking

The drawback of NSEC is that it permits DNS enumeration method called Zone Walking or Zone Enumeration. NSEC records point from one name to another and this allows enumeration of the whole zone. For example using `dig` tool it is easy to see if a top level domain uses NSEC. In the example below one can see that when that when making a DNS query for a TLD name server (`a.fi`) responsible for top level domain `fi.` the authority section reveals that NSEC3 is used for denial of existence, See section XX.

```
> dig +dnssec @a.fi fi.
---
;; AUTHORITY SECTION:
---
uhirv2ck3kkgn20e3fnqecj1nfu6eeko.fi. 86400 IN NSEC3 1 1 5 7B7EE2F...
---
```

On the other hand, using `dig` to query name server (`a.ns.fi`) responsible for TLD `se.` the authority section reveals that NSEC is used which allows zone walking.

```
> dig +dnssec @a.ns.se se.
---
;; AUTHORITY SECTION:
---
se.   7200    IN NSEC  0.se. NS SOA TXT RRSIG NSEC DNSKEY
---
```

In the previous answer `se.` is the start of an interval and `0.se.` is the end of an interval. Requesting DNSSEC resource records for the domain name `0.se.` one can find out the next domain name:

```
> dig +dnssec @a.ns.se se. NSEC
---
;; ANSWER SECTION:
---
0.se.   7200    IN NSEC  0-0.se. NS DS RRSIG NSEC
---
```

Previous answer reveals that the next interval is from `0.se` to `0-0.se`. Iterating previous procedure and listing the domain names is the operating principle of Zone Walking. To illustrate how easily NSEC can be leveraged to perform zone walking Appendix X presents a small Python script to execute zone walking. An example of an output, starting the enumeration from domain `aftonbladet.se.` is presented below.

```
> python3 zone-walk.py aftonbladet.se. 192.36.144.107

aftonbladet.se.
aftonbladet-cdn.se.
aftonbladet-cloudflare.se.
```

```
aftonbladet5.se.
aftonbladet6.se.
aftonbladeta.se.
aftonbladetbingo.se.
aftonbladetblogg.se.
aftonbladetcasino.se.
aftonbladetdeal.se.
aftonbladetdeals.se.
aftonbladetet.se.
aftonbladetf.se.
aftonbladetg.se.
aftonbladeth.se.
aftonbladethierta.se.
aftonbladetkultur.se.
aftonbladetlive.se.
---
```

3.5.3 NSEC3

NSEC allows zone walking, NSEC3 was to make this harder.

3.6 Brute Forcing

3.7 Online Tools

Few words about online databases.

3.8 Notes

What is DNSDB??

What is HINFO??

UPDATE request.

NXDOMAIN

”DNS is defined in RFCs 1034, 1035, 2181” (Tanenbaum)

Tekstiä ja viittaus [15] toinen viittaus. Joku viittaus [7]. Kolmas viittaus [6] something [2] something.

4 Subdomain Enumeration

5 Enumerating Cloud Services

5.1 Something something

Found some scripts that try to enumerate e.g google cloud buckets or Amazon S3 storages.

5.2 Oma testaus2

hello [4].

5.2.1 Testaus2

kfjdkfjf [10] asasa dflfjdf [8] sdsd. [5] dsdsd [11] dsdsd [14] sdsdsd

5.3 Tämän dokumentin tausta

Tämä on TIK.kand-kurssin LaTeX-pohja, jota voi vapaasti käyttää. Koko zip-paketin voi ladata kurssin Noppa-sivulta `https://noppa.aalto.fi/noppa/kurssi/TIK.kand/materiaali/`. Pura zip-paketti, avaa `main.pdf` ja samalla katso ja muokkaa tex- ja bib-tiedostoja vapaasti. Juuri tämä teksti löytyy tiedostosta `luku_sisalto.tex`. Muutoksen jälkeen voit katsoa tilannetta komentamalla `make` ja mahdollisesti päivittämällä PDF-version (reload). Yritä olla koskematta sty- ja bst-tyylitiedostoihin.

Teksti ja koodi on peräisin TIK.kand-kurssin historiallisesta LaTeX-pohjasta, jota kurssin koordinaattori Jukka Parviainen uudisti tammikuussa 2011. Lisäksi suomen kielen lehtori Sanni Heinzmann on kirjoittanut rakenteellisia vinkkejä luvuittain (tiivistelmä, käytetyt lyhenteet, johdanto, loppuluku, liitteet). Viimeisin päivitys on elokuulta 2014.

5.4 Johdantoluku

Työn ensimmäinen luku on aina johdanto. Kandidaatintyön laajuudessa sitä ei ole tarvetta jakaa alalukuihin, diplomityössä ja muissa isommissa töissä sekä tutkimusraporteissa alaluvut ovat mahdollisia (esim. 1.1 Tutkimusongelma, 1.2 Aineisto ja tutkimusmenetelmä, jne.).

Johdannon tarkoitus on antaa lukijalle heti alussa selvä kuva siitä, mihin kysymykseen työ pyrkii vastaamaan (tutkimusongelma). Tyypillisesti aiheen esittely alkaa sanoilla “Tämä (kandidaatin/diplomi)työ käsittelee...” Johdanto esittelee lyhyesti työn pääpiirteet ja

johdattaa lukijan itse työn pariin. Johdannon ohjepituus on 1–3 sivua, kandidaatintyössä 2 sivua on hyvä maksimi.

Käsittele nämä aiheet johdannossa (jotakuinkin tässä järjestyksessä):

- Johdatus aihepiiriin (ei liian laajasti, vaan relevantisti ja napakasti)
- Tutkimuskohteen esittely (MITÄ tämä työ tutkii? Kerro työstä/tutkimusaiheesta, ei omasta kirjoitusprosessistasi tai omasta kiinnostuksestasi.)
- Tutkimuksen perustelu: ongelma tai aukko (aiemmassa tutkimuksessa on aukko, tai siitä nousee esiin kysymys, johon tässä etsitään vastausta)
- Tutkimusongelma / -kysymykset (koko työsi sydän, jonka pitäisi näkyä ”punaisena lankana” koko työn läpi)
- Tavoitteet (Käytä konkreettisesti sanaa ”tavoite”)
- Rajaus (Mitä tämä työ EI tutki)
- Menetelmä, aineisto, teoreettinen kehys (Esittele, MITEN em. aihetta tutkitaan)
- Tulokset? (Johdannossa on ihan hyvä antaa lyhyesti tietoa päätuloksista, mutta ei pakko)
- Työn sisältö ja rakenne (Esittele, miten työn punainen lanka etenee, viittaukset työhön: “ensin, sitten, seuraavaksi, luvussa 3” jne.)

6 Kandidaatintyön rakenne- ja muotoseikat

Tässä luvussa esitellään kandidaatintyön muotovaatimuksia tällä kurssilla. Muutamat alkuperäiset lähteet ovat saattaneet kadota organisaatio- ja tietojärjestelmämuutoksissa, kun Into-järjestelmä on korvannut WWW-sivustoja.

6.1 TKK:n kandidaattityöryhmän ohjeistus

Yleiset kandidaatintyön muotovaatimukset on annettu TKK:n kandidaattityöryhmän päätöksellä 14.11.2006 ja ne ovat kokonaisuudessaan saatavissa osoitteessa `http://www.tkk.fi/fi/opinnot/opintohallinto/paatokset/kandi20061114.pdf`. Tässä luvussa annetaan lyhyt, selvennetty ja joiltakin osiltaan karsittu yhteenveto kyseisistä ohjeista. Seuraavassa viitataan siis edellä mainittuihin TKK:n kandidaatintyön ohjeisiin (esim. “luku 3” tarkoittaa TKK:n kandidaatintyön ohjeiden lukua kolme).

TIK.kand suositus: Lue alkuperäiset ohjeet erityisesti silloin, jos et kirjoita työtä annettua LaTeX-pohjaa käyttäen.

TKK:n kandidaatintyön ohjeissa käsitellään työn rakennetta (luvussa 3) ja muotoseikkoja (luvussa 4). Yleisesti todetaan kandidaatintyöstä seuraavaa:

> *Kandidaatintyö voi perustua teoreettisen taustan tarkasteluun ja sen analysointiin sekä johtopäätösten tekoon tai kokeelliseen osioon ja tulosten analysointiin sekä johtopäätösten tekoon tai edellisten yhdistelmään. Kandidaatintyön rakenteen tulee olla hyvän tieteellisen kirjoittamisen käytännön mukainen ja sisältävän vähintään seuraavat osat: [...] (Luku 3)*

Rakenteen osia ovat: nimiölehti, tiivistelmä, sisällysluettelo, symboli- ja lyhenneluettelo (työn luonteen vaatiessa voi puuttua), johdanto, aikaisempi tutkimus (työn luonteen vaatiessa teoreettinen tausta), tutkimusongelma ja -menetelmät, tulokset, tarkastelu (työn luonteen vaatiessa johtopäätökset tai näiden yhdistelmä), lähteet, liitteet (jos tarpeen). Osat johdannosta tarkasteluun muodostavan työn tekstiosan. (Luku 3) Tekstiosan sopiva pituus on 15–20 sivua eikä työtä ole syytä tarpeettomasti pidentää (luku 4.2.1). Kokonaissivumäärä tulee tällöin olemaan noin 18–25 sivua.

Muotoseikoissa TKK:n kandidaatintyön ohjeissa otetaan esille, että työn tulee olla jäsennelty ja tyylillisesti sekä kielellisesti viimeistelty ja moitteeton. Tarpeettomia tyylillisiä erikoisuuksia tulee välttää. Tekstiosassa tulee olla vain työn kannalta oleelliset kuvat tai taulukot. (Luku 4.1) Kirjasinlaji tulee olla roomalaistyyppinen (Times New Roman tai Computer Modern[1]) ja kooltaan 12 pistettä (luku 4.2.2). Työn nimessä ei saa esiintyä lyhenteitä, kaavoja tai lainauksia (luku 4.2.3).

Nimiölehdellä tulee olla tiedot yliopistosta, tutkinto-ohjelmasta, työn nimestä, luonteesta ("Kandidaatintyö"), päivämäärä ja tekijän nimi (luku 4.2.4). Tiivistelmäsivusta esitetään vastaavat seikat, jotka löytyvät myös tarjolla olevista pohjista (doc[2] tai tämä LaTeX-pohja). Se ei saa olla sivua pidempi. Tiivistelmässä ilmoitettavaan sivumäärään lasketaan kaikki sivut yhteen nimiölehdestä lähdeluettelon tai liitteiden loppuun (Kirjaston suullinen ohje 29.8.2011).

Asemoinnin suhteen tekstiosaa ei sisennetä vaan kappaleiden väliin jätetään yksi tyhjä rivi. Jos oikea reuna tasataan, niin tulee käyttää tavutusta ja tarkistaa, että se menee oikein. Rivivälin tulee olla 1 tai 1,5. (Luku 2.4.7)

Huomaa, että TKK:n kandidaatintyön ohjeissa sivujen numeroinnin ohjeet ovat ristiriitaiset (luku 4.2.6). Oikea sivunumeroinnin malli on toteutettu tässä pohjassa.

Lähdeviittaukset tulee tehdä huolellisesti ja samanmuotoisesti joko nimi-vuosi- tai

[1] LaTeXin perusfontti

[2] `http://peppi.hut.fi/pub/kandi/kandi.php`

numerojärjestelmällä. Alaviitejärjestelmää ei suositella. (Luku 2.4.8)

TIK.kand suositus: Numerointi aloitetaan arabialaisilla numeroilla nimiölehdestä kuitenkin niin, ettei numeroa kirjoiteta sille. Siten ensimmäisen tiivistelmäsivun sivunumero on 2. Kirjasinkoko on 12, riviväli 1,5. Tekstiviitteissä käytetään nimi-vuosi-järjestelmää, mutta tässä ohjaajan sana on määräävä.

6.2 TIK.kand: kommentteja rakenne- ja muotoseikoista

Tekstiasun viimeistelyyn tulee varata runsaasti aikaa V3- ja V4-palautusten väliin. Työn tulisi olla oleellisesti valmis jo V3-palautuksessa, jotta ohjaajasi voi antaa palautetta, kuinka työ viimeistellään ja saadaan hyväksi kokonaisuudeksi, ja sinulla on tarpeeksi aikaa hienosäätöön.

Huomaa, että sivumäärä on hyvin riippuvainen tekstin luonteesta: pelkkää tekstiä mahtuu tässä LaTeX-pohjassa sivulle noin 300 sanaa, kun taas jos mukana on kuvia, luetteloita tai paljon väliotsikkoja, sanamäärä on huomattavasti pienempi. Vastaavasti pienempi riviväli tai fonttikoko antaa lisää sanoja sivua kohden.

Luennolla 6.9.2011 kurssin vastuuopettaja Tomi Janhunen linjasi, että sivumäärä ei ole kriittisin asia vaan itse aiheen käsittely. Jos sivumäärä poikkeaa, ohjaaja tai kurssin henkilökunta voi puuttua tilanteeseen. Jos sivumäärä on pieni, voidaan kysyä, onko aihetta käsitelty tarpeeksi laajasti tai onko selittämiseen tai perusteluihin käytetty vaivaa. Toisaalta iso sivumäärä voi kertoa siitä, ettei työn rajaamista ole hallittu, ja tämäkin voi olla arviointiin liittyvä tekijä. Myöskään ei saa ajatella sitä, että kun 20 sivua tekstiä tulee täyteen, niin opinnäytetyö on valmis. Tieteellisen tekstin kirjoittaminen on iteratiivista: kirjoitetaan, luetaan, karsitaan ja lisätään, kirjoitetaan uudestaan, luetaan, jne. Tyypillisesti sivumäärän kanssa ei tule ongelmaa: annetusta tehtävästä tällä aikataululla tulee tyypillisesti noin 20 sivun mittainen raportti.

Ohjeita kandidaatintyön eri osien kirjoittamiseen on sisällytetty tähän pohjaan. Kirjoittamisohjeita on koskien tiivistelmää, käytetyt lyhenteet -osiota, johdantoa, loppulukua ja liitteitä. Lisäksi lähdekoodissa `main.tex` on ohjeita alkusanoihin, joiden käyttöä ei suositella kandidaatintyössä. .

6.3 Kirjallisuutta

Seuraavat kolme kirjaa löytyvät T-kirjaston käsikirjastosta:

- Kielenhuollon opas tarjoaa apua oikeinkirjoitukseen. Kirjaa saa Kotimaisten kielten tutkimuskeskuksen verkkokaupasta `http://www.kotus.fi/index.phtml?s=2420` 20 euron hintaan.

Kurssiesitteeessä Nopassa on myös linkkejä lukuisiin kotimaisiin Internet-sivustoihin opinnäytetyön kirjoittamisesta. Näitä ovat mm.

- Oulun yliopiston "Kirjoittamisen ABC" `http://webcgi.oulu.fi/oykk/abc`
- Helsingin yliopioston puhe- ja kirjoitusviestinnän opas "Kielijelppi" `http://www.kielijelppi.fi/`
- Oman kirjastomme tarjoama tiedonhaun itseopiskelupaketti `http://peppi.hut.fi/pub/opetus/tiedonhaku/pmwiki.php`
- Yucca Korpela on kirjoittanut nettioppaan "Arkisen asiakirjoittamisen opas" `http://www.cs.tut.fi/~jkorpela/kirj/`
- Aalto-yliopiston Opiskelutaidot-sivusto `https://into.aalto.fi/display/fiopiskelutaidot/`

7 Esimerkkejä LaTeXin käytöstä

Tässä luvussa annetaan esimerkkejä tyypillisimpiin kirjoitustehtäviin. Katso siis valmista PDF-tiedostoa ja lähdetekstiä tiedostossa `luku_sisalto.tex`. Katso myös varsinaista päätiedostoa `main.tex` ja etenkin sen alkua, jossa ladataan lisäpaketteja (sisältäen komentoja). Tämän dokumentin sivuasettelut tehdään pääosin tyylitiedostossa `aaltosci_t.sty`, jota ei tulisi itse muuttaa lainkaan.

Tarkempia ohjeita voi etsiä kirjallisuudesta tai Internetistä sopivilla hakusanoilla. Apua suomeksi: , Wikibooksin LaTeX-opas[3], Jukka Korpelan LaTeX-sivut[4] yms. Järkäleteoksia, mm. on saatavilla myös kirjaston sivujen kautta e-kirjana. Googlaamalla "latex <ongelmasi avainsanoja>" löytyy varmasti apua.

7.1 LaTeXin asennus ja taustaa

TeX-jakeluita on saatavilla "kaikkiin" eri ympäristöihin. Suositeltavaa (helpointa?) on käyttää koulun omia Linux-ympäristöjä, jolloin tarvittavat tausta-asetukset lienevät kunnossa. Windows- ja Mac-koneille on saatavana eri TeX-jakeluja, mm. TeXlipse[5] (Eclipsen liitännäinen) ja MiKTeX[6].

[3] http://en.wikibooks.org/wiki/LaTeX/
[4] http://www.cs.tut.fi/ jkorpela/softa/latex.html
[5] `http://texlipse.sourceforge.net/`
[6] `http://miktex.org/`

7.1.1 Lähdetiedostosta PDF:ksi

Tässä zip-paketissa on mukana `Makefile` (päivitä omat tex- ja bib-tiedostojen nimet), joten pelkkä komento `make` riittää. Olkoon tässä päätiedoston nimi `main.tex` – voit sen vaihtaa luonnollisesti miksi tahansa.

Jos ajat LaTeXia komentoriviltä tai jostain graafisesta ikkunasta, niin "käännä ja kaulitse" `pdflatex main.tex` tarvittaessa kaksikin kertaa. Kun olet lisännyt tekstiviitteitä komenna `pdflatex main`, `bibtex main`, `pdflatex main`, `pdflatex main`. Tarkkaile ruudulle tulevaa tulostusta; esimerkiksi:

```
Package natbib Warning: Citation(s) may have changed.
(natbib)                Rerun to get citations correct.
```

Käännösvaiheissa hakemistoon ilmestyy monenlaisia työ- ja lokitiedostoja, joiden päätteinä mm. aux, log, toc, bbl, blg. Joskus voi olla syytä poistaa nämä komentamalla `make clean`.

7.1.2 Ongelmien ratkaisija: LaTeX checker

Sopiva tekstieditori (emacs, TeXLive, LEd, ...) osaa neuvoja, kun joku tekstissä on joku kielioppivirhe. Tämän lisäksi oiva työkalu on `lacheck`, joka löytyy (?) unix-koneista asennettuna ja ladattavissa Windows-koneelle[7]. Komennon `lacheck main.tex` (`lacheckw32 main.tex`) tulostuksesta voi helposti etsiä, missä kohtaa on jäänyt joku sulku tai ympäristö sulkematta kiinni. Alla olevassa uksessa vika löytyy rivin 224 läheisyydestä.

```
** luku_sisalto:
"luku_sisalto.tex", line 178: missing `\ ' after "engl."
"luku_sisalto.tex", line 224: <- unmatched "\end{center}"
"luku_sisalto.tex", line 1: -> unmatched "beginning of file luku_sisalto.tex"
"luku_sisalto.tex", line 506: <- unmatched "end of file luku_sisalto.tex"
"main.tex", line 48: -> unmatched "\begin{document}"
```

7.1.3 "Ääkköset eivät ole enää ongelma"

Katso tiedoston `main.tex` alkua. Näppäimistön merkistökoodaus valitaan kohdassa `inputenc`. Kaikkien lähdetiedostojen tulee olla saman merkistökoodauksen mukaisia. Useat editorit osaavat vaihtaa koodausta; pääosin on tarve vaihtaa ISO-8859-1 (Latin

[7] `http://www.ctan.org/tex-archive/support/lacheck/`

1) ja UTF-8 (Unicode) välillä. Linuxissa voit katsoa tiedoston koodauksen `file -i tiedosto.tex` ja muuttaa sen tarvittaessa
`iconv -f ISO_8859-1 -t UTF8 fileLatin1.tex > fileUTF8.tex`.

Kohdassa `fontenc` kerrotaan, millaista ulostuloa `pdflatex`in halutaan antavan. Tämä näkyy esimerkiksi siinä, ovatko kirjaimet bittikarttoja vai vektorigrafiikkaa (suurenna PDF-selaimessa 1600%) tai miten ääkköset esitetään (kopioi ja liitä tekstiä ruudulta tekstieditoriin; näkyykö ä `ä`:nä vai `\"a`:na.

Tämän zip-paketin tiedostot ovat UTF8-koodattuja.

7.1.4 Tavutus ei toimi?

LaTeX osaa tavuttaa melko lailla oikein, kun valitaan `babel`illa oikea kieli. Joidenkin hankalien sanojen osalta voit auttaa ehdottamalla tavurajoja paikallisesti `ta\-vu\-ra\-ja` tai koko tekstin osalta `\hyphenation{}`-määrittelyssä `main.tex`:n alussa. Jos tavutus ei toimi, varmista merkistökoodaus (UTF-8 / ISO-8859-1). Varmista myös, että valittuna tekstissä oikea kieli komennolla `\selectlanguage`.

Testaa myös kääntöä IT-keskuksen koneissa – jos toimii koululla, niin omasta jakelusta puuttuu `babel`. Katso myös luvun 7.1.6 `sloppypar`-ympäristö.

7.1.5 Oikoluku

Oikoluvun suoran tuen puute on yksi iso ongelma kirjoitettaessa suomeksi. Yksi mahdollisuus on kopioida teksti johonkin oikolukijaan. Helpompi tapa lienee kopioida tiedostot Linux-koneille, joissa suomenkielisen tekstin voi oikolukea Voikkoa käyttäen tex-tiedostoista `tmispell -dsuomi -t main.tex`. Ohjelman `tmispell` vipu `-t` jättää LaTeX-komennot huomioimatta. Ohjelma saattaa lukea vain UTF8:aa, joten tällöin tiedostot on muutettava tai kopioitava `iconv`illa, katso ääkköslukua yllä.

7.1.6 Hienosäätö

Vihoviimeisen version osalta tulee tarkastaa mm. tavutus (luku 7.1.4) ja rivien siisti ulkoasu. Jos rivillä on kaavoja tai eri fontteja, rivi saattaa jatkua pitkäksi. Tällöin yksi mahdollisuus on käyttää `sloppypar`-ympäristöä, joka antaa LaTeXille lisää vapautta päättää sanojen väleistä (katso lähdekoodi). Komento `\sloppy` antaa väljyyden koko tekstiin. `\hyphenpenalty`-arvon määrittämisen pitäisi myös auttaa (?).

Jos luvun N kuvat tai taulukot "valuvat" lukuun $N + 1$, voi luvun loppuun kokeilla `\clearpage` tai `\afterpage{\clearpage}`, minkä tarkoituksena pakottaa kelluvat objektit tulostumaan ennen luvun loppua.

7.1.7 Eräs vaihtoehto Win7-koneella: MiKTeX ja LEd, Notepad++

Esimerkin omaisesti esittelen oman kokonaisuuteni, johon kuuluu Windows 7 -koneella MiKTeX ja LEd-editori[8]. Jos kaikkia paketteja (engl. package) ei ole ladattu valmiiksi, niin ne kannattaa hakea erikseen MiKTeX package managerilla, joka löytyy nimellä `mpm`.

Ongelmia ja ratkaisuja: Jos paketti on puuttunut ja LEdin kautta lataus epäonnistuu, niin avaa `mpm` ja lataa sitä kautta. Jos tavutus ei toimi, niin tarkista, että sopiva `miktex-hyphen`-paketti on ladattu ja lisäksi suomen kieli on valittu MiKTeXin konfiguraatiossa.

Usein kirjoitan tekstiä Notepad++-editorilla[9], joka on avoimen lähdekoodin ohjelma. Sen jälkeen kopioin tiedoston koulun koneelle, jossa ajan komennon `pdflatex` tai `make`.

7.2 Tekstin kirjoittaminen

Voit kirjoittaa tekstisi suoraan `main.tex`-tiedostoon tai vaikkapa luvuittain omiin tiedostoihin, jotka voi upottaa päätiedostoon `\input`-komennolla. Tässä käytetään dokumenttityyppiä `article`, joka on monessa suhteessa kevyempi ja sopivampi kuin `report` tai `book`.

7.2.1 Perusteksti ja muotoilut

Perusteksti kirjoitetaan konstailematta samalla fontilla ja koolla läpi dokumentin. Sanojen **vahvistamista** tai *kursivointia* tulee välttää. Riviväli on oletusarvoisesti 1,5, mutta sen voi halutessaan vaihtaa väliksi 1 kommentoimalla `main.tex`in alussa `linespread`-rivin. Fontin koko, 12 pt, on asetettu heti `main.tex`:n alussa `\documentclass`-määrittelyssä.

Lainatun tekstin tulee erottua selkeästi omasta tekstistä. Lainauksia tulee käyttää maltillisesti. Asiat tulisi kertoa aina omin sanoin. Lainaus merkitään tyypillisesti tekstin seassa lainausmerkkeihin, jotka kirjoitetaan tyypillisesti kahdella erillisellä merkillä `''` tavallisten lainausmerkkien `"` sijaan. (Ainakin) emacs osaa muuttaa automaattisesti lainausmerkin oikeanlaiseksi. Isompi lainaus voidaan sijoittaa `quotation`-ympäristöön:

> *IP Datacasting is a service where digital content formats, software applications, programming interfaces and multimedia services are combined through IP (Internet Protocol) with digital broadcasting [**?**].*

Prosenttimerkkiä (%) eikä mitään sen oikealla puolella olevaa tulostu ulostuloon. Sillä voi katkaista pitkän rivin ja jatkaa seuraavalta (katso lähdetiedostoa!). Yhdysmerkki

[8] `http://www.latexeditor.org/`
[9] http://notepad-plus-plus.org/

eli yhdysviiva (-) saadaan yhdellä, ajatusviiva (–) kahdella peräkkäisellä yhdysmerkillä: 7–9-vuotiaat, LaTeXin käyttö – helppoa vai hullun hommaa, 25-vuotias.

7.2.2 Luetelmat

Älä käytä luetelmia jatkuvasti kandidaatintyössäsi. Kirjoita mieluummin suoraa tekstiä.

LaTeXin peruslistaympäristöt ovat `itemize`, `enumerate` (numeroitu) ja `description`. Listoja ja niiden ulkoasua on mahdollista muokata [katso esim. **?** , s. 128]. Perusesimerkkejä:

- luetteloaihe yksi
  - luetteloaiheen sisäinen lista
- luetteloaihe kaksi

Toinen luettelo omine merkkeineen:

b) luetteloaihe b

E) luetteloaihe E

Numerointi ympäristössä `enumerate`:

1. luetteloaihe yksi
2. luetteloaihe kaksi

7.2.3 Kuvat ja taulukot

Tyypillisesti kuvat ja taulukot merkitään kelluviksi (engl. float). Tällöin LaTeX järjestää ne sen kannalta parhaaksi katsomiin paikkoihin eikä välttämättä juuri siihen, missä kohtaa kuva tai taulukko on tekstin seassa. Kuvien `\begin{figure}` tai taulukkojen `\begin{table}` määrittelyissä voi kirjoittaa hakasulkuihin `[htb]`, jossa kirjaimet tarkoittavat (h)ere, (t)op, (b)ottom. Kovin yritys pakottaa kuva merkattuun kohtaan on `[h!]`.

Kuvat ja taulukot voi myös sijoittaa suoraan tekstin sekaan, mutta silloin niillä ei ole kuva- tai taulukkotekstejä. Ilman näitä kuvaan tai taulukkoon ei voi viitata tekstistä.

Kuvat kannattaa tallentaa sopivaan formaattiin. Valokuvat JPG ja vektorigrafiikka PDF:nä tai PNG:nä (`pdflatex`). Jos käyttää komentoa `latex` kuvien tulee olla EPS-muodossa (Encapsulated PostScript). Kuvaformaattia voi muuttaa sopivilla kuvankäsittelyohjelmistoilla tai Linux-koneissa esim. `convert`- tai `eps2pdf`-ohjelmilla.

Tässä ensin yksi kuva ja kuvaan 2 viittaminen. Kuva on `figure`-ympäristössä ja siten "kelluva" (float). Englanninkielisessä tekstissä usein isolla alkukirjaimella Figure 2. Kuvatekstin "Kuva" muuttuu sanaksi "Figure", kun valitset kieleksi englannin (`\usepackage[english]{`
Kuvan kokoa voi säätä optiolla `width` tai `height`.

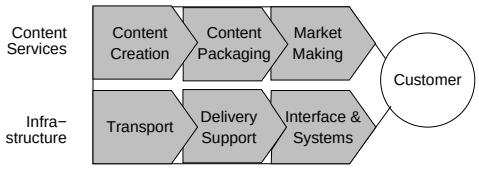

Figure 2: INDICAn kaksitasoinen arvomalli.

Periaatteessa samaan kelluvaan objektiin voi laittaa useammankin kuvan (kuva 3) tai asetella niitä taulukoilla. Jos tarvitset useita kuvia rinnakkain, harkitse myös pakettia `subfigure`. Kuvien olisi hyvä olla samankokoisia.

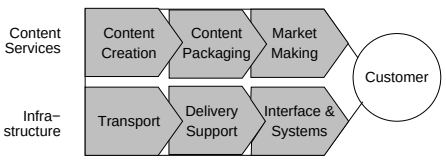

Figure 3: Kaksi kuvaa rinnan esimerkkinä.

Yksinkertainen taulukko, joka ei ole kelluva ja siten sen pitäisi latoutua heti tämän tekstin alle. Tässä komento `\topcaption` kyllä varaa itselleen "Taulukko 1", mutta tekstiä ei näy missään.

Tässä	sarakkeet	ei ole eroteltu mitenkään
ja	ne	saattavat valua yli laidankin ikävästi

Toinen kelluva perustaulukko, viitataan nyt taulukkoon 3. Lähdetekstiä lukiessa näet tilde-merkin, joka pakottaa välilyönnin mutta estää rivinvaihdon.

Table 3: Tässä perustaulukko.

Tässä	sarakkeet	ei ole eroteltu mitenkään
ja	ne	saattavat valua yli laidankin ikävästi, siksi käytä taulukkoa 4. Teksti katoaa jonn
Nro	Nro	Nro
−4	8	12

Vielä kolmas esimerkki taulukosta, jossa sarakkeiden leveys määritelty ja soluissa voi olla useampi rivi tekstiä. Katso taulukko 4.

Table 4: The DVB-T transmission parameters.

Parameter	Typical values
Physical channel	8 MHz (also 6 MHz or 7 MHz possible)
COFDM mode (number of subcarriers, subcarrier width, signal element length)	8k (6817, 1116 Hz, 896 μs) or 2k (1705,4464 Hz, 224 μs)
Guard interval (8k/4k duration)	1/4 (224/56 μs), 1/8 (112/28 μs), 1/16 (56/14 μs) or 1/32 (28/7 μs)
Inner code rate	1/2, 2/3, 3/4, 5/6 or 7/8
Signal element constellation	QPSK, 16-QAM or 64-QAM

Table 5: Kreikkalaiset kirjaimet

α	θ	o	τ	β	ϑ	π	υ
γ	γ	ϖ	ϕ	δ	κ	ρ	φ
ϵ	λ	ϱ	χ	ε	μ	σ	ψ
ζ	ν	ς	ω	η	ξ		
Γ	Λ	Σ	Ψ	Δ	Ξ	Υ	Ω
Θ	Π	Φ					

7.2.4 Matematiikka

Lyhyet matemaattiset kaavat voi kirjoittaa tekstin sisään $E_{\mathrm{total}} = m_i c^2$, mutta kaavat, joita käytetään, kannattaa keskittää

$$x^2 + y^2 = 1 \tag{1}$$

josta lyhyempi versio ilman kaavan numerointia

$$x^2 + y^2 = 1$$

tai jakaa useammalle riville

$$\begin{aligned} x^2 + y^2 &= 1 \\ x &= \sqrt{1 - y^2} \end{aligned} \tag{2}$$

Kreikkalaiset kirjaimet löytyvät taulukosta 5.

Matematiikkaan liittyviä ohjeistusta löytyy esim. **?**]. Makroja sisältävästä tiedostosta `makroja.tex` löytyy joitakin esimerkkejä, kuten

$$\int_{-\infty}^{0} e^x \,\mathrm{d}x$$

7.2.5 Algoritmit ja ohjelmalistaukset

Työlle oleellisen tulostuslistauksen voi laittaa `verbatim`-ympäristöön.

```
Output written on main.pdf (23 pages, 268760 bytes).
Transcript written on main.log.
```

Algoritmien ja pseudokoodin esittämiseen tarvitaan esimerkiksi `algorithmic`- ja `algorithm`-paketit. Ohjelman esittelyn voi tehdä vaikkapa `program`-paketin avulla. Ohjelmakoodia ei tyypillisesti lisätä edes liitteeksi. Jos näin kuitenkin tehdään, käytä ylläolevia tai esimerkiksi `listinginput`-komentoa. Näiden käyttöön löytyy apua Internetistä.

7.3 Viittaukset ja lähdeluettelo

7.3.1 Ristiinviittaukset

Ristiinviittauksia taulukkoon, kuvaan, kappaleeseen tai muuhun voi tehdä `\ref`-komennolla, kuten tässä kuvaan 2. Isossa työssä voi olla näppärä antaa selailun nopeuttamiseksi myös sivunumero: kuva 2 löytyy sivulta 24. Tilde-merkki pakottaa välin, mutta sitoo sen niin, etteivät ne esiinny eri riveillä.

Johdantoluvun lopussa tyypillisesti esitellään kirjan rakenne, joten voi viitata, että luvussa 7.2.2 tarkastellaan sitä ja tätä, luvussa 7.3.3 tuotakin. Englanniksi kirjoitettaessa isolla etukirjaimella “Figure 2 on page 24” ja “Section 7.3.3”.

7.3.2 Lähdetiedosto

Lähdeluettelo kirjoitetaan joko käsin tai automaattisesti kerätyistä lähteistä bib-päätteiseen tiedostoon. Katso esimerkkejä tiedostosta `lahteet.bib`, jota kutsutaan `main.tex` tiedoston loppupuolella.

Kirjaa tiedot mahdollisimman täydellisesti. Kiinnitä erityisesti huomio nimiin ja kirjoita ne samanmuotoisesti `Sukunimi, Etunimi and Sukunimi2, Etunimi2 Etukirjain2.`.

Jos esimerkiksi kirjojen nimissä on muotoiluja, pakkaa ne kaarisulkuihin `{My {T}hesis}`. Pelkkä `title={My Thesis}` muuttuu muuten muotoon “My thesis”.

Kurssilla opetetaan käyttämään RefWorksia lähteiden kokoamiseen. Sieltä on mahdollista saada BibTeX-muotoinen luettelo lähteistä. Valitse ylävalikosta “Bibliography” ja ensimmäisellä kerralla valitse alasvetovalikosta “Access output style manager” ja sieltä lisää BibTeX suosikkeihin. Määrää lähdetiedosto tekstityyppiseksi (“Text”) ja luo tiedosto. RefWorksin tulostukseen tulee loppuun ylimääräinen sulkumerkki `}`, viimeisen

tietorivin perässä ylimääräinen pilkku ja alusta puuttuu itse viittausnimi, jonka voit itse keksiä.

Google Scholar palauttaa myös BibTeX-muotoisia lähdeviitteitä, kunhan olet sen asetuksissa valinnut BibTeXin mahdolliseksi.

7.3.3 Tekstiviite

Tässä pohjassa käytetään Helsingin yliopiston `tktl`-tyyliä, joka pohjautuu `alpha`- ja `natbib`-tyyliin [**?**]. Tekstiviitteet saadaan mukaan joko tekijä-vuosi-tavalla (oletusarvo) tai yksinkertaisella numeromerkinnällä, kuten `[1]`. Jälkimmäistä varten sinun pitää vaihtaa tekstiviitteen esitystapa tiedon `main.tex` lopussa rivillä `bibpunct`.

Katso eri tapoja tekstiviitteiden muotoiluun sivulta `http://merkel.zoneo.net/Latex/natbib.php`. Viittauskomennot `\citet` ja `\citep` ovat hyviä tekijä-vuosi-tavassa `natbib`iin liittyen ja `\cite` on perusviittauskomento.

Pari esimerkkiä: **?** , s. 21] on havainnut asian jos toisenkin. [3] Tämä ja tuo uusi havainto on vahvistanut teoriaa [3, s. 22]. Joku asia on selitetty tarkasti monissa lähteissä [katso **?** , s. 27].

`tktl`-tyylin lähdetiedostoa `tktl.dtx` ei ole muokattu Aalto-yliopiston käyttöön, joten esimerkiksi lähdeviitteen merkintätyyppi `@MasterThesis` tuottaa lähdeluetteloon tekstin "Pro gradu" (kts. `finnbst.tex`). Tämä voidaan muuttaa antamalla kyseisen merkintätyypin kentälle `type` arvo "Diplomityö".

7.3.4 Lähdeluettelo

Lähdeluettelon tulisi nyt ilmaantua dokumentin loppuun automaattisesti. Jos sitä ei näy ja etenkin jos tekstiviitteiden paikalla on kysymysmerkkejä, niin muista ajaa `bibtex main`.

8 Testi: pelkkää tekstiä

Eduskunnan ympäristövaliokunta ehdottaa, että nykyinen hajajätevesiasetus kumotaan ja ympäristöministeriö laatii uuden asetuksen mahdollisimman pian. Lisäksi valiokunta ehdottaa, että ympäristönsuojelulakiin sisällytetään uusi 3 a luku, johon tulee yhteensä 5 pykälää. Ympäristövaliokunta antoi asiaa koskevan mietinnön 25. tammikuuta (YmVM 18/2010).

Valiokunta esittää lisäksi eduskunnan hyväksyttäväksi viisi lausumaehdotusta, joilla vauhditetaan lain ja uuden asetuksen selkeää ja tehokasta toimeenpanoa. Nyt esitettävät

muutokset on valmisteltu tiiviissä yhteistyössä ympäristöministeriön kanssa. Ympäristövaliokunta on käsitellyt asiaa laajasti ja perusteellisesti sekä ottanut ehdotuksissaan huomioon sen, mitä perustuslakivaliokunta aiemmin asiassa edellytti.

Ehdotetuilla muutoksilla kohtuullistetaan hajajätevesien käsittelyn vaatimustasoa siten, että vaatimukset asettuvat yleisesti sellaiselle tasolle, että ne ovat kohtuullisella investoinnilla ja toimivalla tekniikalla moitteettomasti täytettävissä. Esitetty kohtuullistaminen ei kuitenkaan vaaranna ympäristönsuojelun tasoa ja on esimerkiksi Itämeren suojelukomissio HELCOMin suositusten mukainen.

Nykyisen asetuksen lievempi vaatimustaso (orgaaninen aine 80%, kokonaisfosfori 70%, kokonaistyppi 30%) säädetään pääsääntöisesti noudatettavaksi lähtökohdaksi, koska suuri osa kiinteistöistä sijaitsee muualla kuin herkillä alueilla kuten ranta-alueella. Kunnat voivat kuitenkin ympäristönsuojelumääräyksillä antaa tiukempia määräyksiä ympäristön pilaantumisvaaran perusteella herkillä alueilla kuten ranta-alueilla tai tärkeillä pohjavesialueilla.

Puhdistustasovaatimuksen perusteista säädetään laissa ja prosentit edelleen asetuksella. Uudet säännökset ovat ensisijaisesti jätevesijärjestelmän suunnittelun ja rakentamisen lähtökohta, eivät valvontaperuste. Tosiasiallinen puhdistustulos voi siten vaihdella esimerkiksi sääoloista tai kiinteistön käytön väliaikaisista muutoksista johtuen, ja silti järjestelmä täyttää lain vaatimukset.

Valiokunta korostaa, että lain ja asetuksen mukaisten vaatimusten toteuttaminen käytännössä edellyttää aina kiinteistökohtaista arviointia. Kiinteistökohtainen neuvonta on siksi järjestettävä valtakunnallisessa ohjauksessa. Valiokunta edellyttää riittävää määrärahaa neuvonnan järjestämiseksi kunnissa. Vaatimustason muutoksella kohtuullistetaan tarvittavia investointeja, mutta säilytetään samalla riittävä ympäristönsuojelun taso. Erityisen tärkeää on ehkäistä lähiympäristön kuten kaivoveden pilaantumista ja muita vastaavia hygieenisiä haittoja.

Muutoksella vapautetaan suoraan lain nojalla lain voimaan tullessa 68 vuotta täyttäneet vakituisesti asuttujen kiinteistön haltijat asetuksen käsittelyvaatimuksista. Vapautus ei koske uudisrakentamista eikä vapaa-ajan asuntoja. Käytännössä toimenpiteitä tarvitaan vesivessalla varustetuilla vapaa-ajan asunnoilla. Valtaosalla vapaa-ajan asuntoja lainsäädäntö ei aiheuta mitään toimenpiteitä.

Muutoksella tarkennetaan, ketkä voivat hakea kunnalta viiden vuoden mittaista vapautusta asetuksen vaatimusten noudattamisesta niin sanotun sosiaalisen suoritusesteen (erityisen vaikeassa elämäntilanteessa olevat kiinteistönomistajat kuten työttömät ja pitkäaikaissairaat) perusteella. Lainmuutos ja uusi asetus voivat tulla voimaan 15.3.2011. Jo rakennetun kiinteistön olemassa olevan jätevesijärjestelmän on täytettävä puhdistustehosta asetetut vaatimukset vuoteen 2016 mennessä.

Suomen Euroopan neuvoston valtuuskunnan jäsenet Kimmo Sasi (kok.) ja Krista Kiuru

(sd.) vaativat parlamentaarisen yleiskokouksen istunnossa, että Kosovossa rikosten uhreina kadonneiden ihmisten kohtalot selvitetään.

Yleiskokous käsitteli tiistaiaamuna etukäteen paljon huomiota herättänyttä sveitsiläisen kansanedustajan Dick Martyn raporttia Kosovon vuoden 1999 sodan jälkimainingeissa tapahtuneista ihmisoikeusloukkauksista. Martyn mukaan Kosovon vapautusarmeija surmasi vangeiksi ottamiaan ihmisiä, poisti heiltä elimiä ja kauppasi niitä pimeillä markkinoilla.

Keskustelussa Martyn väitteet myös kiistettiin. Kansanedustaja Krista Kiuru korostikin täysistuntopuheessaan, että väitteet pitää tutkia huolellisesti. Totuuden selvittämiseksi tarvitaan puolueeton ja läpinäkyvä tutkinta kansallisten ja kansainvälisten viranomaisten yhteistyönä, hän totesi. Kansanedustaja Kimmo Sasi (kok.) piti huolestuttavana, että satojen ihmisten epäillään kadonneen sodan jälkimainingeissa rikoksen uhreina.

Tarpeellisia selvityksiä ei voida tehdä ilman Albanian ja Kosovon täydellistä yhteistyötä. Euroopan neuvoston pitääkin varmistaa, että selvityksiä ei estetä tai vaikeuteta poliittisista syistä. Kosovon hallitukselle onkin tärkeää, että asia tutkitaan. Vaikeidenkin historian tapahtumien täydellinen läpikäynti auttaa rakentamaan parempaa tulevaisuutta. Osoittamalla olevansa vahva oikeusvaltio, vahvistaa Kosovo omaa asemaansa itsenäisenä valtiona, Sasi totesi.

Eduskunta korjaa pikavauhtia neljän kansanedustajan lakialoitteella metsälakiin jääneen virheen, jonka takia pienet taimikot jäivät tilapäisesti hirvivahinkokorvausten ulkopuolelle. Metsälain muutos tuli voimaan vuoden vaihteessa. Maa- ja metsätalousministeriössä lain valmistelussa tapahtuneen teknisen virheen takia pienet, alle 1,3 metrin pituiset taimikot jäivät lakimuutoksen myötä hirvivahinkojen korvauksen ulkopuolelle. Lakitekstiin kiireessä jäänyt virhe havaittiin vasta, kun laki oli jo hyväksytty ja vahvistettu, mitä ministeriö pahoitteli. Virhe korjataan eduskunnan maa- ja metsätalousvaliokunnan puheenjohtajan Jari Lepän (kesk.) lakialoitteella, jonka on allekirjoittanut myös kolme muuta valiokunnan kansanedustajaa.

Aloitteen tekijät ehdottavat, että kyseistä riistavahinkolain pykälää korjattaisiin siten, että lakia sovellettaisiin taannehtivasti vuoden alusta alkaen. Siten kukaan ei lopullisesti menetä oikeuttaan korvaukseen. Lakialoite (LA 121/2010) oli lähetekeskustelussa tiistaina. Keskustelun päätteeksi asia lähetettiin maa- ja metsätalousvaliokuntaan.

Euroopan unionin ympäristömerkki siirtyy samaan kotipesään pohjoismaisen Joutsenmerkin kanssa. Eduskunta hyväksyi tiistaina lakimuutoksen, jolla ympäristömerkinnän kansallisten tehtävien hoito siirtyy Suomen Standardisoimisliitolta Motiva Services Oy:lle. Suomessa on käytössä kaksi virallista ympäristömerkintäjärjestelmää. Pohjoismainen ympäristömerkki eli Joutsenmerkki on Pohjoismaiden ministerineuvoston vuonna 1989 perustama merkki. EU:n ympäristömerkki on Euroopan parlamentin ja neuvoston antamaan asetukseen

pohjautuva ympäristömerkki.

9 Loppuluku

Loppuluku päättää työn. Luvun nimi on tyypillisesti “yhteenveto” tai “johtopäätöksiä”. Valitse se otsikko, joka tuntuu sopivammalta työsi luonteeseen. Joka tapauksessa loppuluku sisältää niin työn yhteenvedon kuin johtopäätöksiä työn tulosten perusteella. Pääajatus on antaa lukijalle selvä kuva siitä, miten johdannossa asetettuihin tavoitteisiin työssä vastattiin.

Käsittele loppupuvussa seuraavia asioita (jotakuinkin tässä järjestyksessä):

- Muistutus työn tavoitteista (sidoksisuus johdantoon)
- Päätulokset kootaan yhteen, pohditaan niiden merkitystä
- Suositukset konkreettisiksi toimenpiteiksi (“Mitä sitten?” Nyt kun käytössä on tämän työn myötä tullut tieto, mitä se nyt tarkoittaa tälle asialle/alalle.)
- Tulosten soveltuvuus, käyttöön liittyvät rajoitukset
- Jatkotutkimustarve (“Tulevaisuudessa olisi mielenkiintoista selvittää...” tms.)
- Työn onnistumisen arviointi (Huom! Älä arvioi omaa kirjoitusprosessiasi vaan tekemääsi tutkimusta)

10 Liite

```
import dns.resolver
import sys

def walk(start, dns_ip):
    start, end = get_answer(start, dns_ip)
    print(start)
    print(end)
    while True:
        start, end = get_answer(end, dns_ip)
        print(end)

def get_answer(name, dns_ip):
    req = dns.message.make_query(name, rdtype=dns.rdatatype.NSEC)
```

```
    response = dns.query.udp(req, dns_ip)

    # Example answer section of a Resource Record of type NSEC:
    #
    #   a.org 7200 IN NSEC b.org NS SOA TXT RRSIG NSEC DNSKEY,
    #
    # where a.org is the start of the interval and
    # b.org is the end of the interval

    answer = response.answer[0].to_text()
    arr = answer.split(' ')

    # return start and end of the interval
    return arr[0], arr[4]

if __name__ == "__main__":
    args = sys.argv[1:]
    walk(args[0], args[1])
```

References

[1] *Network Security Assessment*. O'Reilly Media, Inc., first edition.

[2] Casey Deccio and Jacob Davis. Dns privacy in practice and preparation. *Proceedings of the 15th International Conference on Emerging Networking Experiments And Technologies*, CoNEXT '19, page 138–143, New York, NY, USA, 2019. Association for Computing Machinery. ISBN 9781450369985. doi: 10.1145/3359989.3365435. URL https://doi.org/10.1145/3359989.3365435.

[3] Kensuke Fukuda and John Heidemann. Detecting malicious activity with dns backscatter. *Proceedings of the 2015 Internet Measurement Conference*, IMC '15, page 197–210, New York, NY, USA, 2015. Association for Computing Machinery. ISBN 9781450338486. doi: 10.1145/2815675.2815706. URL https://doi.org/10.1145/2815675.2815706.

[4] Kimberly Graves. *CEH Certified Ethical Hacker Study Guide: Certified Ethical Hacker Study Guide*. John Wiley & Sons, Incorporated, Hoboken, 2010. ISBN 9780470525203.

[5] A. Klein, H. Shulman and M. Waidner. Counting in the dark: Dns caches discovery and enumeration in the internet. *2017 47th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, pages 367–378, 2017. doi: 10.1109/DSN.2017.63.

[6] Maciej Korczyński, Michał Król and Michel van Eeten. Zone poisoning: The how and where of non-secure dns dynamic updates. *Proceedings of the 2016 Internet Measurement Conference*, IMC '16, page 271–278, New York, NY, USA, 2016. Association for Computing Machinery. ISBN 9781450345262. doi: 10.1145/2987443.2987477. URL https://doi.org/10.1145/2987443.2987477.

[7] James F. Kurose and Keith W. Ross. *Computer networking : a top-down approach*. Pearson, Boston, 2013. ISBN 9780273775638.

[8] Daiping Liu, Shuai Hao and Haining Wang. All your dns records point to us: Understanding the security threats of dangling dns records. *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, CCS '16, page 1414–1425, New York, NY, USA, 2016. Association for Computing Machinery. ISBN 9781450341394. doi: 10.1145/2976749.2978387. URL https://doi.org/10.1145/2976749.2978387.

[9] Paul Mockapetris. RFC 1035: Domain Names - Implentation And Specification, November 1987. Status: DRAFT STANDARD.

[10] Jeffrey Pang, Aditya Akella, Anees Shaikh, Balachander Krishnamurthy and Srinivasan Seshan. On the responsiveness of dns-based network control. *Proceedings of the 4th ACM SIGCOMM Conference on Internet Measurement*, IMC '04, page 21–26, New York, NY, USA, 2004. Association for Computing Machinery. ISBN 1581138210. doi: 10.1145/1028788.1028792. URL `https://doi.org/10.1145/1028788.1028792`.

[11] Tommi Piipponen. Laitteiden ja palvelujen löytäminen ipv6-verkossa. Kandidaatintyö, Aalto-yliopiston perustieteiden korkeakoulu, Espoo, 2011. Saatavissa `http://urn.fi/URN:NBN:fi:aalto-201305162358`. Viitattu 2.2.2020.

[12] Haya Shulman and Michael Waidner. One key to sign them all considered vulnerable: Evaluation of DNSSEC in the internet. *14th USENIX Symposium on Networked Systems Design and Implementation (NSDI 17)*, pages 131–144, Boston, MA, March 2017. USENIX Association. ISBN 978-1-931971-37-9. URL `https://www.usenix.org/conference/nsdi17/technical-sessions/presentation/shulman`.

[13] M. Skwarek, M. Korczynski, W. Mazurczyk and A. Duda. Characterizing vulnerability of dns axfr transfers with global-scale scanning. *2019 IEEE Security and Privacy Workshops (SPW)*, pages 193–198, 2019. doi: 10.1109/SPW.2019.00044.

[14] Joni Taipale. Palvelun löytäminen erilaisissa verkoissa; service discovery in different networks. Kandidaatintyö, Aalto-yliopiston perustieteiden korkeakoulu, Espoo, 2011. Saatavissa `http://urn.fi/URN:NBN:fi:aalto-201305162355`. Viitattu 2.2.2020.

[15] Andrew S. Tanenbaum and D. Wetherall. *Computer networks*. Pearson, Harlow, fifth edition, 2014. ISBN 9781292037189.