LAB06 Nettverksovervåking med Wireshark

Daniel Eide, Jørgen Lybeck Hansen, Jonas Dam, Elaine Sajets, Christian Fredrik Thorne, Bastian Strang

Dato: 15.03.2015

Versjon 1.0

Kurs: IS-105

# Oppgave 1

**A)**

Hvor lang tid tok det fra ”http GET”-meldingen ble sendt til ”http OK” ble mottatt, og hva kan man bruke denne verdien til? (Verdien av ”time”-kolonnen er antall sekunder som er gått etter at du startet capture)

## HTTP GET

Meldingen ble sendt 4.42 sekunder etter capture:

*18 4.425417000 10.0.0.3 216.58.209.110 HTTP 1206 GET /complete/search?q=http%3A%2F%2Fwww-net.cs.umass.edu%2F HTTP/1.1*

## HTTP OK

Ble mottatt 4.55 sekunder etter capture:

*22 4.559675000 216.58.209.110 10.0.0.3 HTTP 537 HTTP/1.1 200 OK*

*Time since request: 0.136361000 seconds*

Tiden imellom disse HTTP protokollene betyr hvor lang tid nettverket bruker på å sende ut og å motta svar på forespørsler. Her ser vi at forskjellen bare er 0.13 sekunder (4.55 - 4.42).

Vi legger merke til at Source og Destination bytter plass.

**B)**

Utvid alle feltene under "Hypertext Transfer Protocol" i det midterste vinduet. Forklar hva de forskjellige feltene brukes til. Bruk verdiene dere har fått i wireshark som eksempel. Gjør dette for både HTTP GET og HTTP OK.

<https://wiki.wireshark.org/Hyper_Text_Transfer_Protocol>

***HTTP GET***

*Host:* [*http://www-net.cs.umass.edu*](http://www-net.cs.umass.edu/)

- Denne forteller adressen til noden vi prøver å kontakte

*Connection: Keep-alive*

- Dette er en melding som er sendt fra en enhet til en annen for se at linken mellom de to enhetene kjører, eller for å forhindre at denne linken brytes

*Cache-Control: Max-age=0*

- Den sjekker om du har cache fra før av lagret I nettleseren og kan tvinge ny cache om det kommer en ny oppdatering til nettsiden. Det er ofte gitt en tid før du trenger å få en ny cache. Hvis meldingen er http 200 ok har den hentet cache om det står not modified 304 har den hentet cachen du har fra før av

*Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,\*/\*;q=0.8*

- Forteller oss om hvilkne content-typer som er akseptert

*User-Agent: Mozilla/5.0 (X11; Linux x86\_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/40.0.2214.115 Safari/537.36*

- Denne forteller om User-Agent identifikasjon, den forteller hvilket software, operativ system den bruker osv

*Accept-Encoding: gzip, deflate, sdch*

- Gir oss informasjon på hvilken enkoding som er akseptert

*Accept-Language: en-US,en;q=0.8*

- Forteller oss om menneskelige språk som er tillatt å få respons I fra

***HTTP OK***

*Cache-Control: no-cache, no-store, must-revalidate\r\n*

- Forteller browseren hva den har tillatelse til å cache på nettsiden.

*Content-Type: image/gif\r\n*

- MIME-type - Internet Media Type. Brukes for å identifisere hva slags media som er på nettsiden.

*Expires: 0\r\n*

- Dato/tid på når responsen på forespørselen skal stoppe.

*Pragma: no-cache\r\n*

- Et felt som er basert på en spesifikk implementasjon. Kan ha forskjellig effekt i forskjellige punkter av request-response kjeden.

*Content-Length: 43\r\n*

- Lengden på pakken oppgitt i bytes.

*Connection: keep-alive\r\n*

- Dette er en melding som er sendt fra en enhet til en annen for se at linken mellom de to enhetene kjører, eller for å forhindre at denne linken brytes

*Time since request: 0.260645000 seconds*

- Tiden det tok å få et svar fra vi sendte HTTP GET forespørselen.

# Oppgave 2

## IF-MODIFIED-SINCE

Under HTTP protokollen kan vi lese av IF-MODIFIED-SINCE visst vi har lastet inn siden på nytt. Wireshark ser at nettsiden er vært på tidligere og gir oss informasjon om dette.

**Denne HTTP protokollen er fra første lasting av nettsiden:**

*30 6.371888000 158.37.245.96 128.119.245.12 HTTP 515 GET /ethereal-labs/HTTP-ethereal-file2.html HTTP/1.1*

**Denne er neste opplasting som kommer 2.29 sekunder senere:**

*50 8.687348000 158.37.245.96 128.119.245.12 HTTP 627 GET /ethereal-labs/HTTP-ethereal-file2.html HTTP/1.1*

**Under den siste “pakken” kan vi lese av if-modified-since pakken:**

*If-Modified-Since: Mon, 16 Mar 2015 05:59:02 GMT\r\n*

Setningen forteller oss 2 ting: Om nettsiden har endret seg og om noe har endret seg så nettsiden må lastes ned på nytt med ny informasjon.

**A)**

Som forklart vil ikke IF-MODIFIED-SINCE være med i første GET forespørsel. Det er fordi den ikke er registrert fra før og har ingen tidspunkt å være modifisert siden.

**B)**

Responsen på GET forespørselen sier oss at vi får en text/html fil, som var det vi forespurte.

Dette sier oss at det er en text/html fil

*Content-Type: text/html; charset=UTF-8\r\n*

Siden vi lastet inn nettsiden 5 ganger er vår HTTP response på 1/5 ved første OK, 2/5 ved andre, 3/5 ved tredje osv.

**C)**

Siden vi oppdaterte nettsiden 5 ganger har vi flere GET forespørsel pakker. Alle sammen har en lik IF-MODIFIED-SINCE linje som sier oss at visst noe har skjedd siden første gang nettsiden ble lastet inn så må den lastes inn på nytt. Denne nettsiden har ikke endret seg noen gang gjennom oppdateringene så vi får likt tidspunkt overalt.

*If-Modified-Since: Mon, 16 Mar 2015 05:59:02 GMT\r\n*

**D)**

I infoen på oppdaterte pakker ser vi at istedenfor OK, får vi Not Modified. Dette betyr at nettsiden ikke er endret på (og ikke krever oppdatering) siden sist vi var her. Dette er et resultat av cache.

Før Not Modified har vi en response code som sier 304. Dette kan sammenlignes med Error 404 som også er en type response code. 304 betyr at nettsiden allerede er lastet inn og ikke endret siden sist, så ingen endringer trenger å gjøres før den lastes inn på nytt.

*51 8.895849000 128.119.245.12 158.37.245.96 HTTP 308 HTTP/1.1 304 Not Modified*

## Her er noen eksempler på source codes:

* 304 Not Modified
  + Indicates that the resource has not been modified since the version specified by the [request headers](http://en.wikipedia.org/wiki/List_of_HTTP_header_fields#Request_Headers) If-Modified-Since or If-None-Match. This means that there is no need to retransmit the resource, since the client still has a previously-downloaded copy.
* [403 Forbidden](http://en.wikipedia.org/wiki/HTTP_403)
  + The request was a valid request, but the server is refusing to respond to it. Unlike a *401 Unauthorized* response, authenticating will make no difference.
* [404 Not Found](http://en.wikipedia.org/wiki/HTTP_404)
  + The requested resource could not be found but may be available again in the future. Subsequent requests by the client are permissible.

# Oppgave 3

Som opplyst får vi ikke en login boks fra denne linken og oppgaven kan ikk løses.