Cybermissionen 2024
Lærervejledning

Victor Hjelmberg Feddersen og Andreas Alstrup

May 2024

Indhold

1 Indledning

1.1 Læringsmål

1. Awareness omkring de informationer du deler eller andre og om dig
2. Basalt kenskab til HTTP/HTTPS netværkspakker
3. Basale færdigheder inden for cybersikkerhed.
4. Kompetencer til at navigere Haaukins på egen hånd.

1.2 Opgaver og løsninger

Opgaverne som er inkluderet i denne cybermission vil herefter blive refereret til som challenges. Der er i alt 9 challenges som er inkluderet i opgavesættet. Rækkefølgen, de er beskrevet i herunder, vil også være den anbefalede, når eleverne skal løse opgaverne. Det er en god ide at lægge små pauser ind undervejs og også at gennemgå nogle af opgaverne løbende så elever ikke sidder fast i en opgave i længere tid. De første 5 opgaver er tiltænkt, som de vigtigste for at nå læringsmålene, som er beskrevet herover:

1. Certified Secrets
2. Meta
3. Peacock: En lang rejse
4. Peacock: OSINT hack
5. Bad librarian

Extra opgaver

6. dotsuffix
7. Dictionary attacks
8. USBestjålet
9. Browserauth

2 Challenges

2.1 Certified Secrets

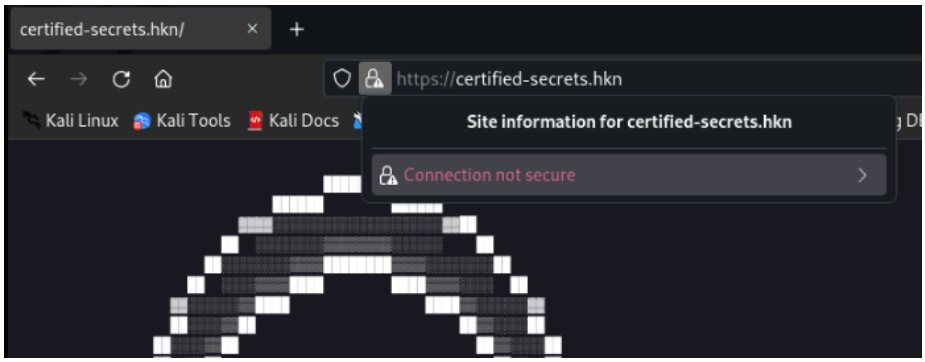
Denne opgave skal give forståelse for hvad et certifikat er og dets rolle i at skabe en sikker udvæksling af information for brugeren. Det er nemlig vigtigt at tjekke om den side man bruger er krypteret (HTTPS), for ellers kan adgangskoder og anden information blive opsnappet af andre der holder øje med ens aktiviteter. På en siden som ikke er krypteret (HTTP) vil ens browser advare som "Ikke sikker". Men også HTTPS sider med et ikke verificeret certifikat advares som "Ikke sikker". Opgaven går ud på at se hvad et certifikat indholder, og et spørgsmål til eleverne kunne være *Hvorfor vises et ikke verificeret certifikat som "Ikke sikkert"*?

2.1.1 Beskrivelse på Haaukins

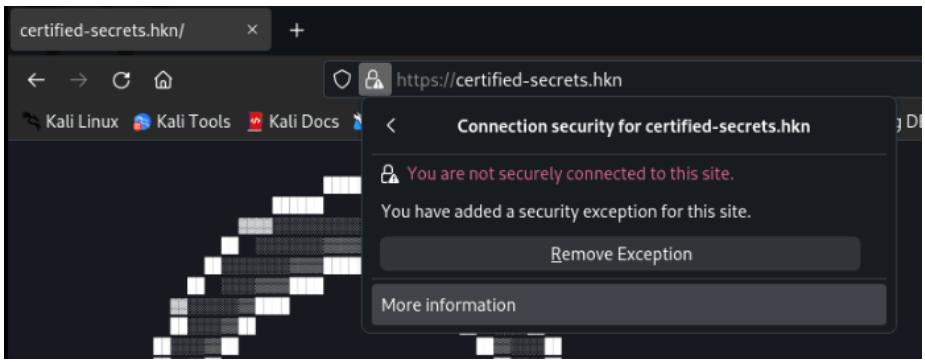
```
Look at this site!
It uses HTTPS! But what does an SSL certificate tell us about the site
https://certified-secrets.hkn
```

2.1.2 Løsning

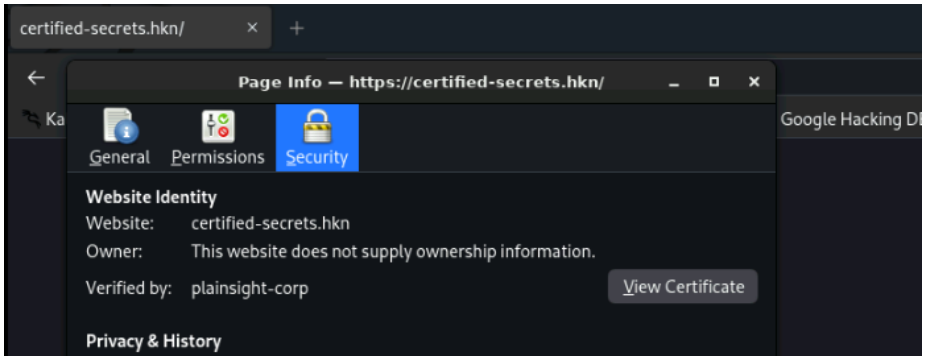
1. Gå til `https://certified-secrets.hkn`. Her vises et hint til en URL sti: `https://certified-secrets.hkn/C/ST/L/O/email/DNS`
2. Klik på låseikonet i venstre side af URL'en, for at se sidens certifikat (se figure 1, 2, 3).
3. Brug informationen til at udfylde URL stien.
   - `C`: dk
   - `ST`: nordjylland
   - `L`: aalborg
   - `O`: plainsight-corp
   - `email`: hidden@pc.com
   - `DNS`: secure.gov
4. Besøg nu det korrekte URL for at få flaget:
   `https://certified-secrets.hkn`
   `/dk/nordjylland/aalborg/plainsight-corp/hidden@pc.com/secure.gov`



Figur 1: Klik på låseikonet.



Figur 2: Klik på "More information".



Figur 3: Klik på "View Certificate".

2.2 Meta

En fil indeholder også information om filen selv. Denne metadata kan blandt andet afsløre hvor og hvornår et billede er blevet taget. Det er godt at vide at denne information følger med i de filer man deler og hvilket digitalt fodspor man efterlader.

2.2.1 Beskrivelse på Haaukins

```
*Category: Forensics*
- Download[1]
- Vi har modtaget dette billede fra vores agent. Han siger, at der
er en hemmelighed gemt inde i den. Kan du finde det?
```

2.2.2 Løsning

1. Download `meta.zip` og udpak den.
2. Læs billedets (`meta.png`) metadata
   - Gå til `https://exif.tools/` (Ikke i Haaukins) og upload billedet
3. Flaget kan ses i `Comment` feltet, `DDC{h1dd3n_1n_m3tad4t4}`.

[1] https://nextcloud.ntp-event.dk:8443/s/53ePbkx23MDPBey/download/meta.zip

2.3 Peacock: En lang rejse

Denne challenge handler om hvordan man kan bruge detaljer i billeder til at finde lokationen hvor billedet er blevet taget. Peacock er et socialt medie hvor folk kan dele billeder og kommentare. Freja Hackmann har delt 3 billeder og ud fra billederne skal man finde ud af hvilke 3 byer hun er i.

2.3.1 Beskrivelse på Haaukins

Vi er igang med at undersøge Freja Hackmann som er en del af en stor international kriminel organisation. Vi kan se at hun har postet feriebilleder fra 3 rejsedestinationer og vi har grund til at tro at hun brugte sin rejse til at kontakte medlemmer fra organisationen. Vi har brug for din hjælp til at finde ud af hvilke byer hun rejste til. Du kan finde hendes profil på http://peacock.hkn

Formen på flaget er: HKN{By1_By2_By3} hvor By1 er navnet på den første by hun rejste til, By2 er den anden og By3 er den sidste. Hvis hendes rejse f.eks. var fra Oslo til Berlin til København ville flaget være HKN{Oslo_Berlin_København} Vær opmærksom på store/små bogstaver.

2.3.2 Løsning

1. Gå til `Freja Hackermanns` profil her kan man højreklikke på billederne og klikke åben i ny fane for at få en større version af dem.

2. På billedet af det første rejsemål, kan man se at bilerne kører i venstre side af vejbanen, derudover kan man se teksten `PARLIMENT SQUARE SW1` som når man googler viser sig at være relateret til London. Bygningen man kan se er `Palace of Westminster` som ligger i London.

3. På billedet af den andede rejsemål, kan man se en cafe som hedder `Crêperie Parisienne`. Googler man den kan man se at den ligger på addressen 18 Quai du Louvre, 75001 Paris, Frankrig. Helt til venstre kan man også se det franske flag, og et ord man ikke kan se det hele af, dog ligner det at der kunne stå Paris.

4. På billedet af det tredje rejsemål kan man længst til højre se det grøndlanske flag. Byen ser relativt befolket ud, hvilket kunne tyde på at det var en af grøndlans største byer, da grøndlands befolkningstal er relativt lavt. Grøndlands største by er Nuuk, og googler man billeder af bygninger i Nuuk kan man finde bygningerne til venstre på billedet ved navn Tuapannguit.

5. Samlet set får man flaget HKN{London_Paris_Nuuk}

2.4 Peacock: OSINT hack

Denne opgave handler om de informationer som folk deler om hinanden. Emilie Netgaard har ikke selv postet noget på det sociale media Peacock andet end et billede af hendes hund, men det har hendes venner og familie. Ud fra oplysninger fra de posts kan man resette hendes password ved at svare på 3 sikkerhedsspsørgsmål. 1. Hvad er hendes fødselsdag, 2. Hvad hedder hendes ynlingskæledyr og 3. Hvad er navnet på hendes folkeskole.

2.4.1 Beskrivelse på Haaukins

Emilie Netgaard har brug for din hjælp. Hun kan ikke huske hendes password, så hun kan ikke længere logge ind. Kan du hjælpe hende?
Du kan finde hendes og andre profiler på http://peacock.hkn

2.4.2 Løsning

1. På loginsiden på http://peacock.hkn kan man se en knap der hedder `Har du glemt et password`. Klikker man på den kan man se at man kan resette sit password hvis man kender fødselsdag, navnet på ynlingskæledyret og hvilken folkeskole Emilie Netgaard gik i.

2. Man kan klikke "Sign up"og oprette sin egen bruger for at kunne se posts.

3. Scroller man gennem postene kan man se et post fra Magnus Cybersen som ønsker Emilie tillyke med fødselsdagen. I kommentarene kan man se at hun er født i 1986 og hun er en måned fra at have fødselsdag d. 1. April, hvilket betyder at hendes fødselsdag er enten 1/3/1986 eller 1/5/1986.

4. I et andet post fra Magnus Cybersen kan man se at hun passer `Fido`, hvilket kunne være hendes kæledyr, måske også det hun selv har lagt et billede op af.

5. Viktor Kodegaard har lagt et billede op hvor han rykker for betailinger til en genforeningsfest for hans folkeskole hvor Emilie er inviteret. Navnet på skolen kan læses i kommentarene: `Engelbjergskolen`.

6. Man kan nu logge ud og gå til password reset siden som i step 1. Her indtaster man `Emilie Netgaard` som navn, et tilfældigt kodeord, fødselsdagen `1/3/1986`, ynlingskæledyret `Fido` og folkeskolen `Engelbjergskolen` så får man derefter flaget `HKN{Hashtag_AltDetViDeler}`. Hvis man indtaster 1/5/1986 som fødselsdag får man en fejlbesked der siger at fødselsdagen er forkert.

2.5 Bad librarian

Det er ikke altid sikkert at begår sig online selv om ens forbindelse er krypteret med HTTPS. For hvis man benytter f.eks en offentlig computer på biblioteket kan en ondsindet person få den computer man bruger til at gemme de TLS keys

som bruges til at krypteres de netværkspakker der senders over HTTPS. En person der har konfiguret en sådan computer på forhånd, vil senere kunne se al den aktivitet man har lavet fra computeren, og ens adgangskoder, bankoplysning ovs. vil f.eks kunne læses af hackeren. I denne opgave ses hvordan dette scenarie kunne udspille sig i praksis. Her for eleverne nemlig adgang til de TLS keys der bruges til at dekryptere de netværkspakker som en computer har sendt over HTTPS og eleverne skal læse HTTPS krypterede chat beskeder.

2.5.1 Beskrivelse på Haaukins

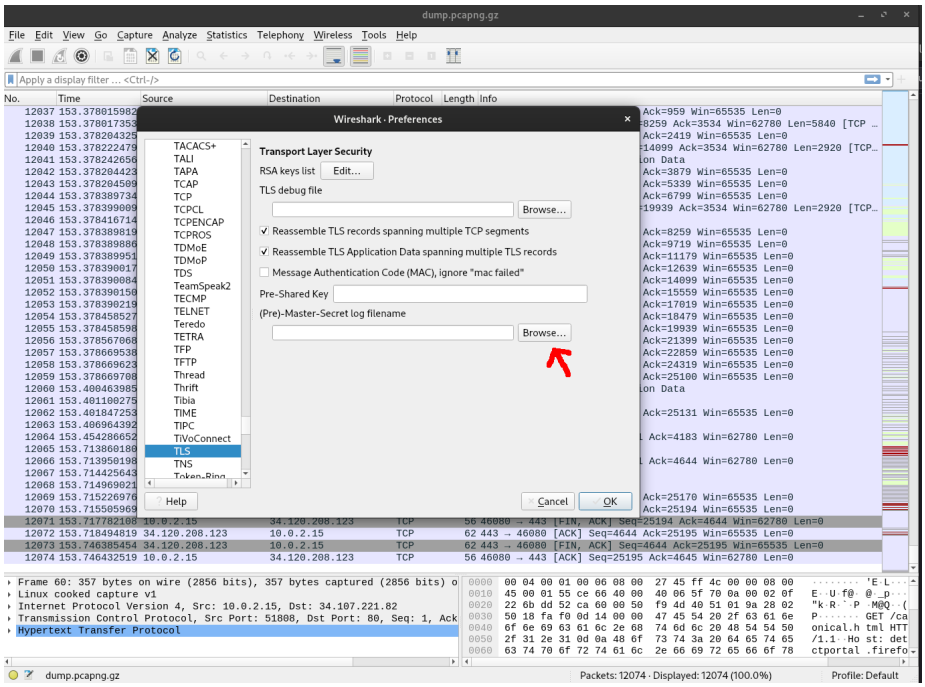
I'm sure library computers are safe to use. But beware of the librarian i have heard she likes to log a lot.

- Download[2] the librarian's files.'

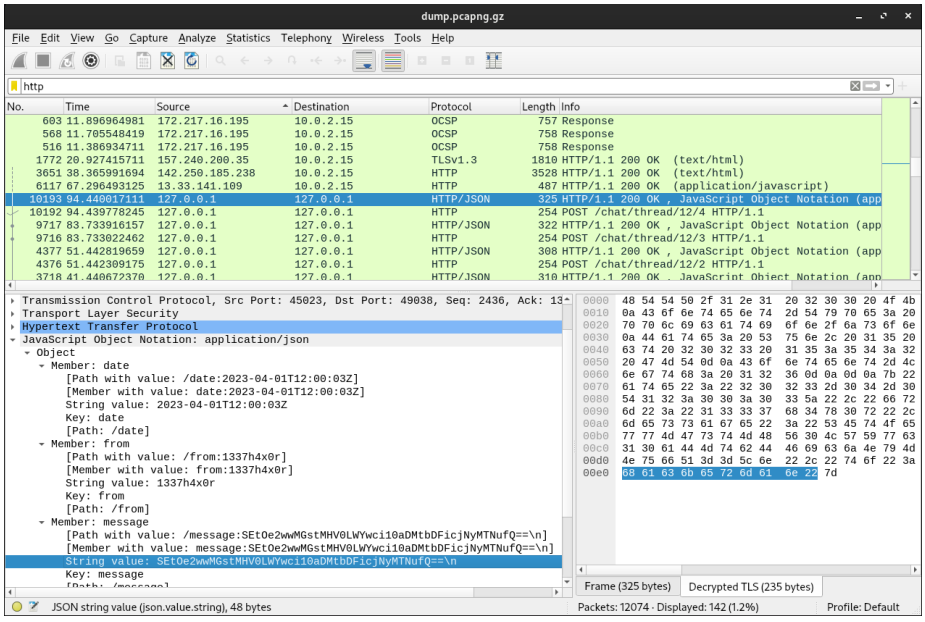
2.5.2 Løsning

1. Åben `dump.pcapng.gz` i Wireshark[3]
2. Wireshark viser nu en liste over netværkspakker hvor mange af dem er krypteret
3. Brug `tlskey.log` til at dekrypter netværkspakker
    - Gå til `Edit->Preferences->Protocols->TLS` og vælg `tlskey.log` (se figur 4)
4. Skriv `http` i Wireshark's `display filter` for kun at se `HTTP` netværkspakker (text input felt øverst i Wireshark *Apply a display filter*)
5. Undersøg dem hvis protocol er `HTTP/JSON`. En udveksling af skjulte meddelelse kan nu ses
6. Få fat i den skjulte meddelse som er `Base64` encoded (se figur 5)
7. Decode `SEtOe2wwMGstMHV0LWYwci10aDMtbDFicjNyMTNufQ==` meddelelsen
    - Brug CyberChef (https://gchq.github.io/CyberChef) til at decode meddelelsen eller Google "decode Base64"
8. Få flaget `HKN{l00k-0ut-f0r-th3-l1br3r13n}` ved at decode `Base64` meddelelsen

[2] `https://nextcloud.haaukins.com/s/wWDrdZFbjoXPb5Y/download`
[3] https://www.wireshark.org/



Figur 4: Dekrypter netværkspakker ved at klik "Browse"og vælg `tlskey.log`.



Figur 5: Undersøg de dekrypteret netværkspakker med `http` som filter og få fat i den sjkulte `Base64` meddelelse.

2.6 dotsuffix

Der findes et utal af file extension f.eks `.txt`, `.pdf`, `.doc`. En file extension er den måde vi navngiver filer på, således at syresystemet ved hvilket program det skal bruge til at håndterer filen. Når vi ændre denne file extension kan syresystemet havde svært ved at forså filen og man kan let tro at filen er beskadiget. Men ved at undersøge filen nærmere kan man finde frem til files rigtige format og se hvad filen indholder.

2.6.1 Beskrivelse på Haaukins

```
Things are never as they seem.
It's always a matter of perspective.
Look carefully at the FILE through the eyes of the terminal.
```
`pokemon.jpeg`[4]

2.6.2 Løsning

1. Download `pokemon.jpg` og opdag at billedet ikke kan åbnes.
2. Åben programmet `Terminal` i Haaukins.
3. Skriv `file pokemon.jpg` lær at filen er af et `Zip archive date` format.
4. Ændre file extension fra `.txt` til `.zip` og uppak nu filen.
5. Et billede af et pokemonkort (`porygon39.jpg`) kan nu åbnes.
6. Flaget er står nederst på pokemonkortet, `HKN{p0ry60n_15_7h3_rul3r_0f_cyb3r_5p4c3}`.

[4] https://nextcloud.ntp-event.dk:8443/s/6aWBjPSSbepcBN4/download/pokemon.jpg

2.7 Dictionary attacks

Når man logger på WIFI sender ens router (access point) en krypteret besked til den enhed man logger in fra og ens enhed svare routeren tilbage. Denne udveksling kaldes et WPA2-PSK handshake og er her routeren og enheden generer nøgler for at oprette en sikker forbindelse fremover. Ved at opfange dette WPA2-PSK handshake, kan en hacker finde frem til WIFI adgangskoden ved at prøve en masse forskellige adgangskoder. En lange list med adgangskoder er den kendte liste `rockyou.txt`, som nemt kan findes i Haaukins eller ved at google "rockyou"på google. Det er derfor vigtigt ikke har have en WIFI adgangkode som let kan gættes ud fra en kendt wordlist så som `rockyou.txt`.

2.7.1 Beskrivelse på Haaukins

`Antallet af usikre wifi-adgangskoder vil ROCK YOU!`
`Se, om du kan bryde wifi-adgangskoden til dette TP-Link-adgangspunkt.`
`Flaget er adgangskoden.`
`Download`[5]
`(Måske du kan nå at drikke en kop kaffe imens din pc arbejder! Eller en hel kande!)`

2.7.2 Løsning

1. Åben `handshake.cap` i Wireshark
2. Wireshark viser nu en liste over netværkspakker hvor vi skal finde MAC addressen på et TP-Link access point.
3. Vi kan se at MAC adressen er `14:eb:b6:86:3c:97` da dette device sandsynligvis er et access point fordi det broadcast'er til andre enheder (Kan ses under kolonne "Destination"i WireShark).
4. Brug værktøjet `Aircrack-ng` med `rockyou.txt` ordlisten til at crack det WPA2-PSK handshake som er WireShark
   - Åben programmet `Terminal` i haaukins
   - Skriv `aircrack-ng -w /usr/share/wordlists/rockyou.txt -b 14:EB:B6:86:3C:97 handshake.cap`
   - Vent på at `Aircrack-ng` er færdig. Men vær tålmodig, det kan tage op til 20 minutter.
   - Herefter får vi WIFI adgangskoden: `dontstealmynameagainyoufreak`
5. Flaget er `DDC{dontstealmynameagainyoufreak}`

[5] https://nextcloud.haaukins.com/s/Y6tMWkyZkoHZnHs/download/crypto-dictattack.zip

2.8 USBestjålet

Det USB image der downloads til opgaven svare til et USB stik der kunne sidde i computeren. Men der er slettet noget fra USB stikket og ved hjælp af et forensic værktøjet kan slettede file gendannes fra dets hukommelse. Dette er teknikker der bruge indenfor politiet og et spørgsmål til eleverne kunne være *Hvordan sletter man noget så der er ingen spor fra det?*.

Hvis eleverne synes det kunne være sjovt at se hvad der ligger på `USB.001` uden først at finde de slettede filer kan de køre `udisksctl loop-setup --file usb.001` i Haaukins og bruge det som var det et normalt USB stik.

2.8.1 Beskrivelse på Haaukins

```
Politiet anholdt i november en ung mand i København og sigtede ham
for at stjæle et hemmeligt dokument fra BBC. Ifølge BBC er det meste
af dokumentet volapyk, men det gemmer på en hemmelighed.

Et USB-stik er under afhøringen af den anholdte blevet beslaglagt og
sendt til teknisk analyse. Politiet har vurderet det meget sandsynligt,
at dokumentet har ligget på USB-stikket og har brug for at finde det
før retssagen. Den tekniske afdeling har dog kun fundet en række Monty
Python memes og et manuskript.

Kan du hjælpe politiet med deres efterforskning?

drive_usb_1gb.zip[6]
```

2.8.2 Løsning

1. Download `drive_usb_1gb.zip` og udpak den.
2. Undersøg nu `usb.001` med et forensic tool, så som `foremost` der er godt til store mængder af data.
3. Åben programmet `Terminal` i haaukins. Skriv derefter `foremost usb.001`.
4. Undersøg nu hvad der ligger i `output` mappen.
5. Udpak `00880064.zip` som ligger i mappen `zip`.
6. Åben `Lorem_Ipsum.rtf` og find en base64 encoded tekst, `RERDezcxNV9idTdfNF81Y3I0N2NofQ==`.
7. Decode `RERDezcxNV9idTdfNF81Y3I0N2NofQ==` i f.eks CyberChef[7] eller google "base64 decode".
8. Flaget er `DDC{715_bu7_4_5cr47ch}`.

[6] https://nextcloud.ntp-event.dk:8443/s/s5HzksPmrQbdkje/download/drive_usb_1gb.zip
[7] https://gchq.github.io/CyberChef/

2.9 Browserauth

BrowserAuth handler om at man skal analysere netværkspakke gennem et værtøj som Wireshark, så man kan finde den URL som indeholder flaget, samt hvilken User Agent man skal have for at tilgå den URL.

2.9.1 Beskrivelse på Haaukins

BrowserAuth the game changing passwordless authenticationmethod without any vulnerabilities... or so they say. Let's prove them wrong. I've captured some interesting packages, that you could try to take a look at.

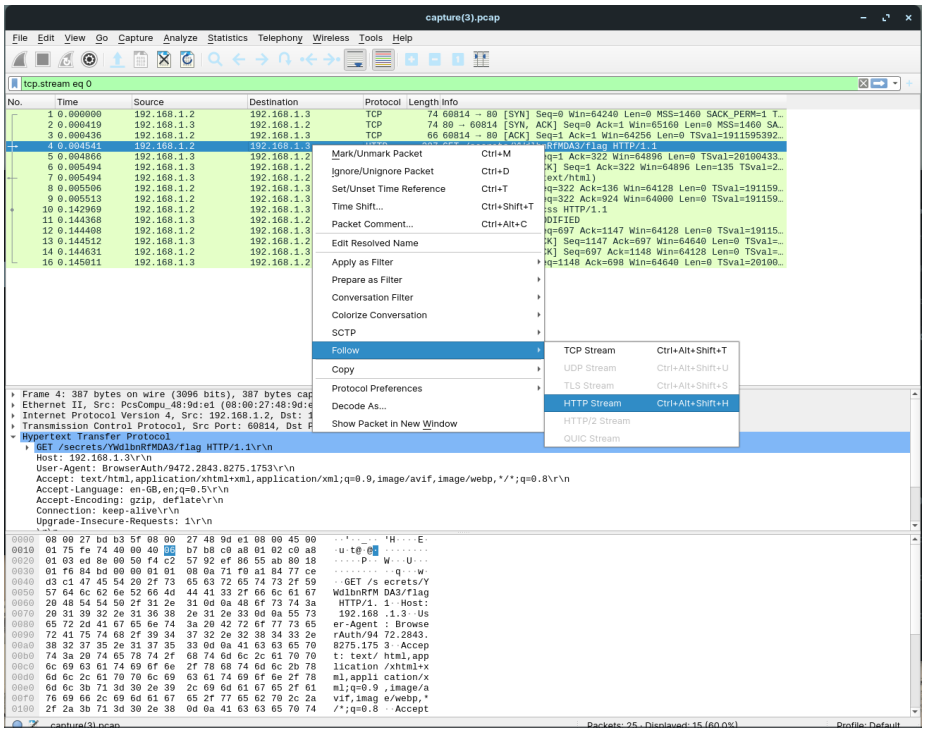
Download[8]

http://browserauth.hkn

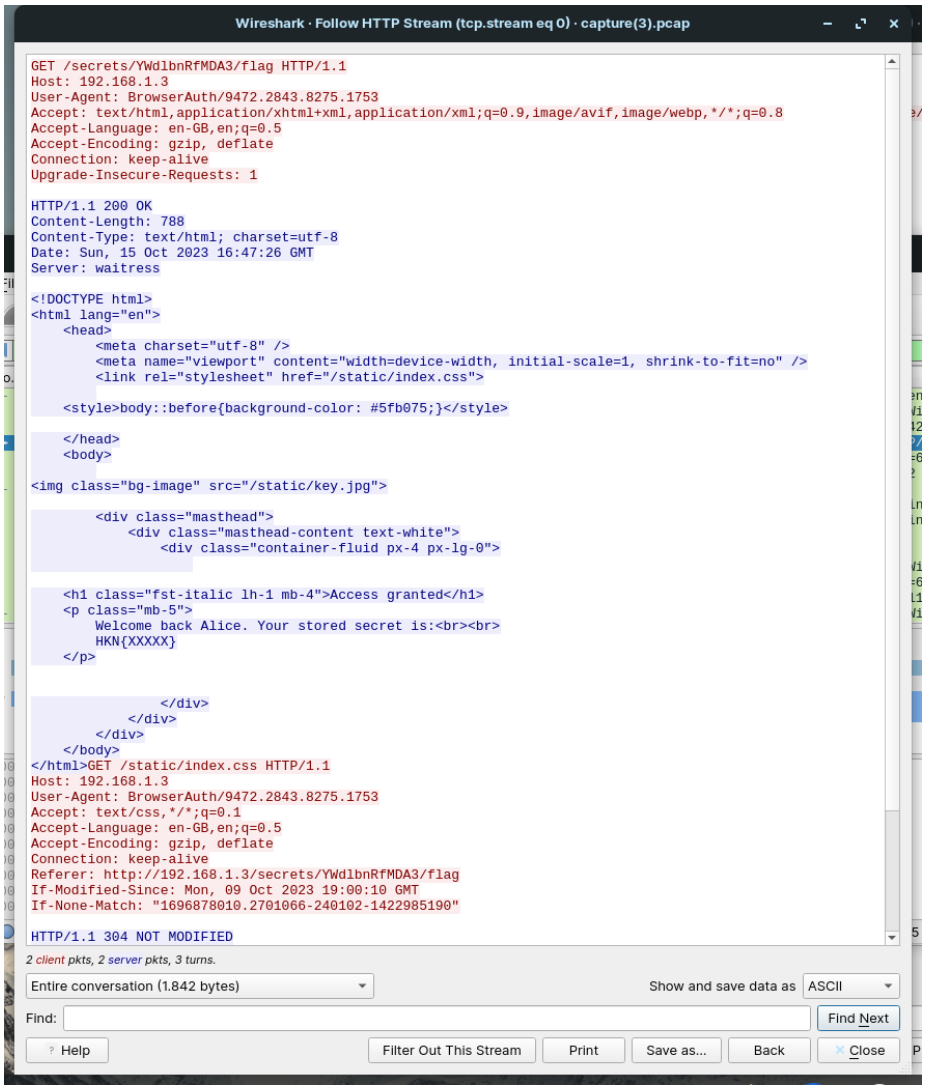
2.9.2 Løsning

1. Download og installer WireShark
2. Åben `capture.pcap` i Wireshark
3. Wireshark viser nu en liste over netværkspakker man kan undersøge.
4. Den 4. pakke er en http pakke. På den kan man `højreklikke` → `Follow` → `HTTP Stream` (Se Figur 6)
5. I det vindue der popper op (Se Figur 7) kan man i de første 3 linjer se "GET /secrets/YWdlbnRfMDA3/flag HTTP/1.1"og "User-Agent: BrowserAuth/9472.2843.8275.1753". Det betyder at der en en der har forsøgt at tilgå http://browserauth.hkn/secrets/YWdlbnRfMDA3/flag med en specefik user agent.
6. Forsøger man at tilgå http://browserauth.hkn/secrets/YWdlbnRfMDA3/flag får man en fejlbesked som siger at man skal have den top hemmelige browser for at kunne tilgå siden. Browsere bruger http headeren "user agent"til at finde ud af hvilken browser man bruger, det kan man dog forfalske.
7. I firefox kan man skifte user agent ved at gå til `about:config` og søg efter `general.useragent.override`. Vælg `String` click på `+` iconet og skriv `BrowserAuth/9472.2843` som vi fandt i tideligere.
8. Nu har du forfalsket din browser til en der kan tilgå siden.
   Gå til http://browserauth.hkn/secrets/YWdlbnRfMDA3/flag og få flaget.
   `HKN{wlerzQMwJIdhTm5WCWbSD}`

[8] https://nextcloud.haaukins.com/s/fxGdBLfADn2kAwN/download/capture.pcap



Figur 6: Skærmbillede af capture.pcap åbnet i Wireshark.



Figur 7: Skærmbillede af "Follow HTTP"lokation.