Documentatie

Versie 2.0

Table of Contents

Over Publeaks

In iedere samenleving vinden misstanden plaats. Tipgevers hebben misschien informatie of kennis van zaken die niet in de haak zijn en waarvan zij vinden dat ze moeten worden onderzocht, om er een einde aan te maken of misschien om er een bredere discussie mee los te maken.

Publeaks is een omgeving die deze tipgevers in staat stelt om veilig en anoniem informatie te lekken naar de pers. De aanbrenger kan zelf selecteren naar welke van de aangesloten mediaorganisaties hij of zij de stukken wil sturen en de ontvangende journalist kan berichten achterlaten voor de aanbieder.

De journalist besluit zelfstandig tot verificatie, nader onderzoek of publicatie. De pers heeft als opdracht om te controleren, om te publiceren, om aan de orde te stellen. De pers is daar toe uitgerust. Journalisten zijn professionals die onderzoeken, doorvragen, wederhoor toepassen en ze hebben een medium waarmee ze zaken naar buiten kunnen brengen.

Natuurlijk is lekken niet zonder risico, maar Publeaks maakt het zo veilig mogelijk. Zo zorgt het systeem er voor dat de afzender, locatie en andere gegevens van het versturen van documentatie niet te herleiden is.

Publeaks.nl is een samenwerking tussen de stichting Publeaks, het Hermes Centrum voor Transparantie en Digitale Rechten, het Internet Protection Lab en Greenhost.

Stichting Publeaks

De Stichting Publeaks wil de journalistieke infrastructuur versterken en het journalistieke vermogen door middel van het ondersteunen van geanonimiseerde communicatie tussen burgers en persorganen.

Het bestuur van de stichting Publeaks.nl bestaat uit:

- Teun Gautier – Directeur De Groene Amsterdammer
- Mieke van Heesewijk – Directeur Netwerk Democratie
- Corine de Vries – Lid van Hoofdredactie De Volkskrant

De stichting heeft geen enkele toegang tot de inhoud van stukken of rol in de relaties tussen journalist en aanbieder van informatie. De stichting heeft slechts tot doel om de infrastructuur beschikbaar te maken. De stichting, noch een andere (rechts-)persoon heeft toegang tot de gegevens op het systeem waar het informatie over aanbrenger betreft of de eventueel verzonden stukken.

De stichting heeft een zeer beperkte begroting die wordt opgebracht door de deelnemende persbedrijven, fondsen en donaties.

Stichting Publeaks is bereikbaar via info@publeaks.nl

Netwerk Democratie

Netwerk Democratie is mede verantwoordelijk voor de idee-ontwikkeling en realisatie van Publeaks.nl. De stichting Netwerk Democratie zet zich in voor een veerkrachtige democratie waarin burgers meer betrokken zijn en, met behulp van technologie, actief bijdragen.

www.netdem.nl

Hermes Centrum voor Transparantie en Digitale Rechten

Het Hermes Centrum voor Transparantie en Digitale Rechten heeft de software Globaleaks ontwikkeld. Globaleaks is een open source project gericht op het creëren van een wereldwijd, anoniem, censuur-bestendig, klokkenluiders platform.

In samenwerking met Publeaks is de Gloableaks software aangepast en vertaald. Het resultaat van die samenwerking is publeaks.nl.

www.logioshermes.org

Het Internet Protection Lab

Het Internet Protection Lab is verantwoordelijk voor het technisch projectmanagement van Publeaks.nl. Het Internet Protection Lab biedt overal ter wereld concrete en gerichte steun aan journalisten, bloggers en activisten die bedreigd worden. Door het bieden van internetverbindingen, expertise van beveiligde webhosting, maken ze hun werk veiliger en effectiever.

www.internetprotectionlab.net

Greenhost

Greenhost is verantwoordelijk voor de hosting en ondersteuning van Publeaks. Naast het aanbieden van duurzame hosting en veilige email steunt Greenhost projecten in onderwijs, cultuur en journalistiek. Ze zetten zich in voor een open en vrij internet en de bescherming van haar gebruikers. Greenhost staat pal voor vrijheid van informatie, privacy en openbaarheid van bestuur.

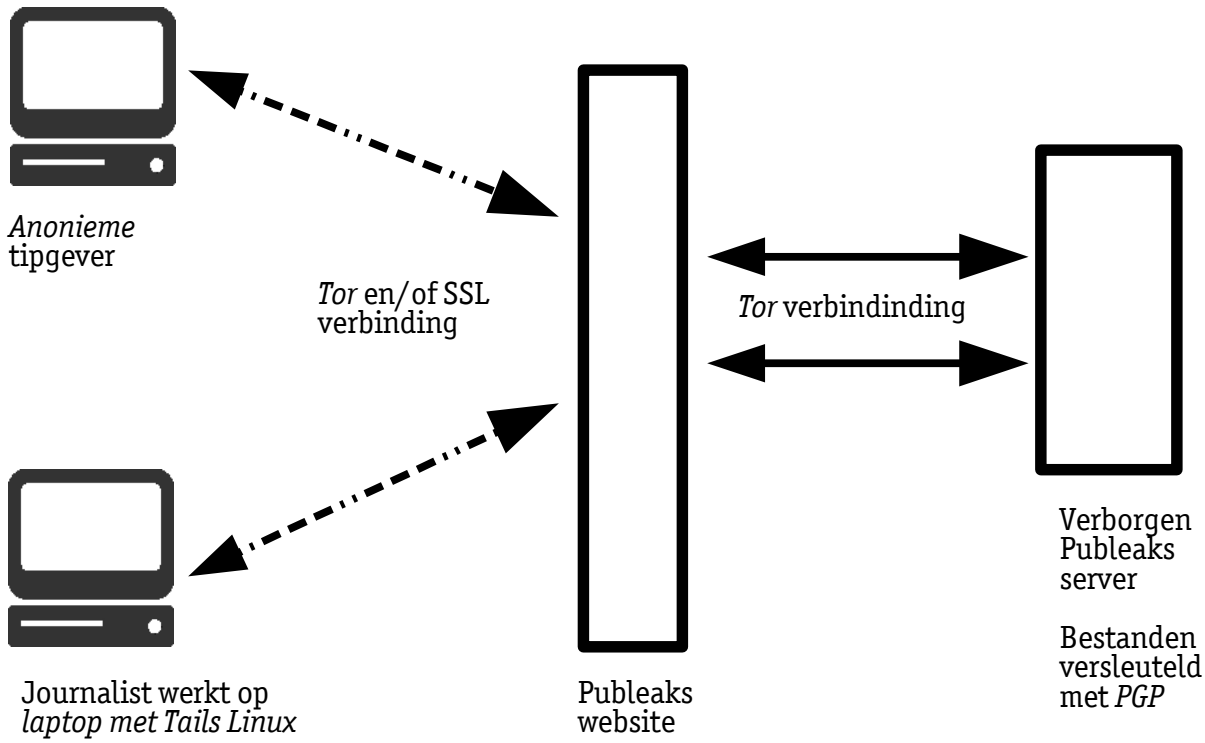
www.greenhost.nl
Tel. 020-4890444

Hoe Publeaks is opgezet

Het platform

Het primaire doel van het Publeaks platform is te zorgen dat de tipgever anoniem kan blijven als hij of zij dat wil. Daartoe is een systeem opgezet dat op verschillende manieren zorgt dat de identiteit van een tipgever niet bekend wordt.

Hierbij moet worden opgemerkt dat geen enkele techniek feilloos is, dus ook die van Publeaks niet. Wel heeft Publeaks, mede door gebruik te maken van de nieuwste technieken, het voor de tipgevers zo veilig mogelijk gemaakt.



Tor en/of SSL verbinding

Een tipgever wordt aangeraden om gebruik te maken van het Tor netwerk. Dit netwerk is opgezet met als doel anoniem op internet te kunnen surfen. (Lees verderop meer over Tor.) De tipgever kan ervoor kiezen Tor niet te gebruiken, dat is aan hem of haar.
De verbinding met Publeaks is, naast eventueel gebruik van Tor, in elk geval altijd beveiligd met SSL. Dus ook als men geen Tor gebruikt en een bezoek niet geheel anoniem is, kan in elk geval niemand zien wát er wordt gelekt.

Verborgen Publeaks server

Publeaks bestaat vervolgens uit twee delen. De 'voorkant' van de website is gewoon bereikbaar via

het normale internet. De 'achterkant' daarentegen, daar waar de alle data wordt opgeslagen, is alleen via Tor bereikbaar. Hierdoor is het op de server aan de 'achterkant' onmogelijk om te achterhalen wie bestanden naar de Publeaks server heeft geüpload.

Daarnaast zorgt het gebruik van Tor er hier voor dat niemand kan achterhalen waar de server fysiek staat, wat toegang krijgen tot de server een stuk moeilijker maakt.

PGP versleuteling van bestanden

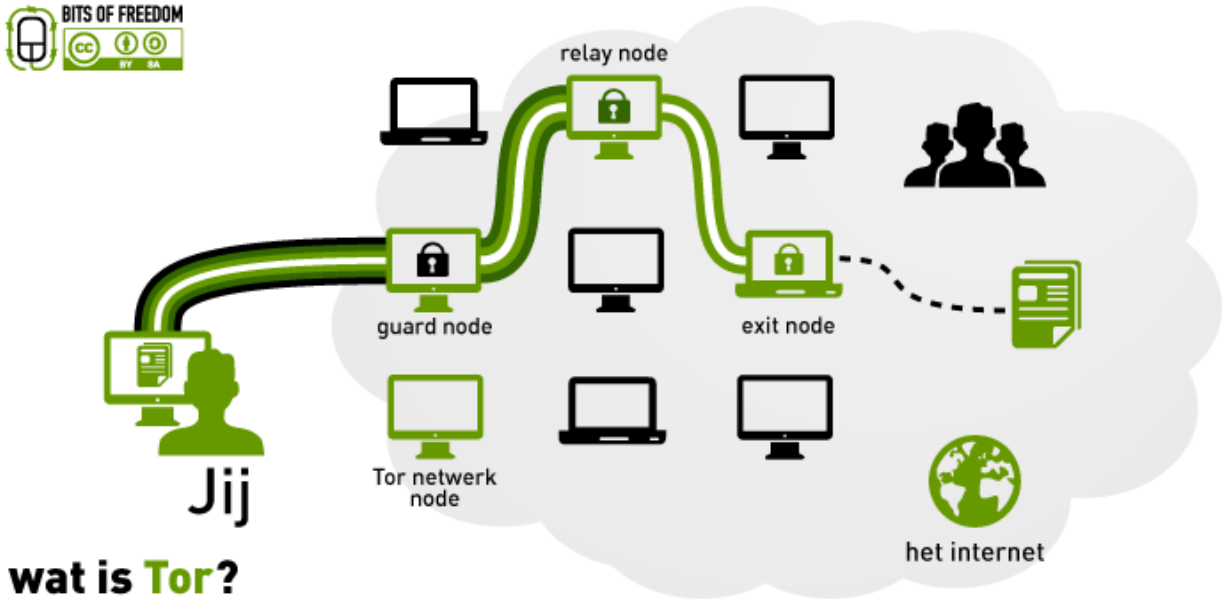
Bestanden die worden geüpload naar de server worden daar versleuteld met PGP opgeslagen. Daarvoor worden alleen die PGP sleutels gebruikt, die horen bij de media waarvan de tipgever heeft aangegeven dat hij er zijn informatie aan wil geven. Dus alleen die media en niemand anders kan de bestanden ontsleutelen.

Journalist werkt op een laptop met Tails Linux

De journalist gebruikt voor het ophalen van de tips een speciaal daarvoor gebruikte laptop met Tails Linux. Deze laptop bied de mogelijkheid om in een veilige omgeving bestanden te anonimiseren voordat ze de wereld in worden gebracht.

Tor netwerk

Tor is een netwerk van vrijwilligers dat gezamenlijk ervoor zorgt dat je anoniem kunt blijven op internet. Het anonimiseren werkt doordat Tor op zijn weg naar het internet eerst driemaal een willekeurige en versleutelde verbinding maakt met een node in het Tor netwerk. De website die wordt bezocht kan daardoor bijna onmogelijk herleiden wie feitelijk de website bezoekt.



PGP encryptie

Is het PGP of GPG? Beide hebben dezelfde oorsprong en dezelfde functionaliteit, maar het belangrijkste verschil is dat PGP betaalde software is en GPG vrij beschikbare open-source software

is. Linux maakt standaard gebruik van de GPG en dus is het commando dat we gebruiken *gpg*. Overigens heet GPG officieel GnuPG.

PGP is een zogenoemde asymmetrische encryptie methode die werkt met sleutelparen. Elk sleutelpaar bestaat uit twee sleuteldelen, een publiek deel en een privé deel. De publieke sleutel wordt gebruikt voor het versleutelen van data en het privé deel voor het ontsleutelen van data.

Het principe werkt zo dat je iemand je publieke sleutel geeft en dat hij of zij die gebruikt om iets te versleutelen. Jij bent vervolgens de enige die deze data met jouw privé sleutel kan ontsleutelen. De data kan dus veilig via het internet naar je worden opgestuurd.

Het is dus van belang dat de privé sleutel veilig wordt bewaard en niet in verkeerde handen valt. Een manier om dat te doen is door een wachtwoord op de privé sleutel te zetten.

Linux distributie Tails

Tails is een Linux versie die speciaal is ontwikkeld om je veilig en anoniem op het internet te begeven. Voor de journalisten is de anonimiteit minder van belang, zij maken er tenslotte geen geheim van dat ze gebruik maken van Publeaks. De extra veiligheid die Tails biedt is wel van belang. In Tails kan namelijk versleuteld data worden opgeslagen en Tails laat geen sporen achter.

Tails wordt gestart van een usb stick en bij het afsluiten wordt alle informatie over wat de journalist heeft gedaan gewist. Op de laptop zijn dus geen sporen te vinden die iets kunnen vertellen over wat de journalist heeft gedaan en welke tips hij mogelijk heeft gekregen. Daarnaast is het veel moeilijker om malware en spyware te installeren, aangezien de laptop telkens schoon opstart.

De laptop biedt ook de mogelijkheid om veilig bestanden en informatie op te slaan in het zogenaamde 'persistent volume'. Dit 'persistent volume' is een versleuteld deel op de usb stick waar Tails een beperkte hoeveelheid data op kan slaan. Onder andere wordt de PGP sleutel hierin opgeslagen.

De laptop kan worden gebruikt om veilig bestanden op te halen, op te slaan en te ontdoen van eventuele (meta)data die de identiteit van de tipgever prijs zou kunnen geven. Voor dat laatste is er speciale software op de laptop aanwezig die de journalist hierbij kan helpen.

Wachtwoord kwijt

Er zitten in PGP en de versleutelde opslag op de Tails usb-stick géén achterdeurtjes of workarounds. Als een wachtwoord kwijt is, dan is daar helemaal niets meer aan te doen. Alle data die dan nog versleuteld is, moet als verloren worden beschouwd.

Wel is het mogelijk een nieuwe publieke sleutel in Publeaks te plaatsen, zodat bij nieuwe tips gebruik wordt gemaakt van een sleutel waar wel toegang toe is. Eventueel kan een tipgever te

vragen de documenten nogmaals te uploaden.

Opdrachten workshop

1. Steek eerst de usb in de laptop en start daarna pas de laptop. Log vervolgens in.
2. Maak een Encrypted persistent volume aan.
3. Herstart en log in met *Use persistent* storage *Yes*.
4. Maak een PGP sleutelpaar aan.
5. Log in op https://secure.publeaks.nl
6. Voeg je aangemaakte PGP key toe aan je *voorkeuren*. (Log daarna uit.)

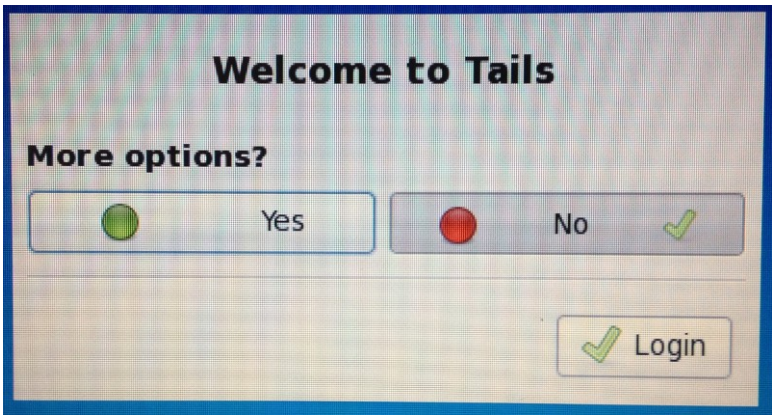
De stappen 1 t/m 6 zijn noodzakelijk om het systeem te configureren en je in staat te stellen tips te ontvangen. De overige stappen zijn interessant als je wilt leren hoe het systeem werkt.

7. Upload een bestand via de website (en sla de code op die je krijgt!)
8. Bekijk de e-mail melding die je binnen hebt gekregen.
9. Log als jezelf in op de website en bekijk de tip die je hebt opgestuurd.
10. Geef een reactie op deze tip.
11. Download het bestand dat je had geüpload en decrypt het op je laptop.
12. Verwijder de metadata van het bestand m.b.v. *Metadata Anonymisation Toolkit*.
13. Lees de reactie die je eerder gaf en schrijf een antwoord terug.
14. Upload een extra bestand. (Log daarna uit.)
15. Bekijk de nieuwe e-mail melding die je binnen hebt gekregen.
16. Log weer als jezelf in en bekijk de gewijzigde tip.
17. Log in als tipgever met de code die je eerder hebt opgeslagen.
18. Download het nieuwe bestand en decrypt het.

Handleidingen receiver

Opstarten laptop en inloggen

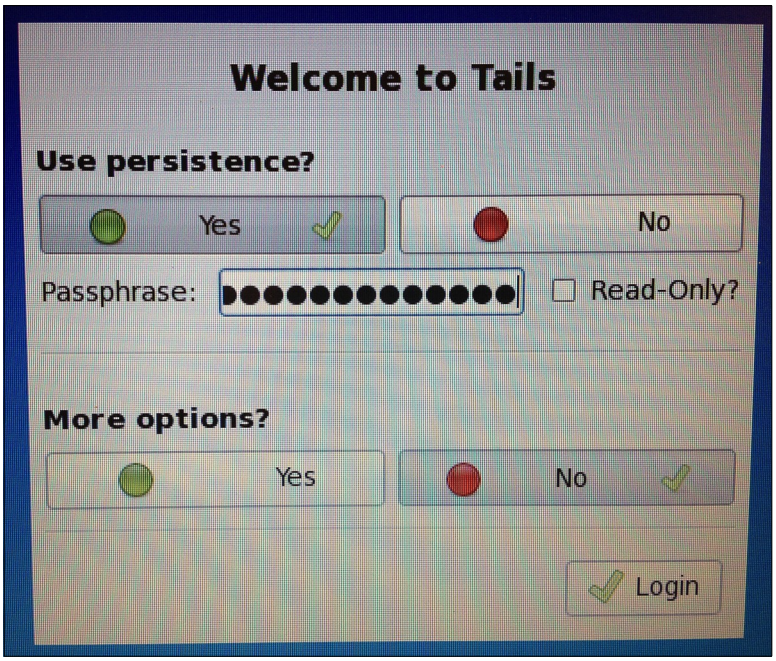
Steek eerst de memorystick met de Linux versie 'Tails' in de laptop en zet daarna pas de laptop aan.



De eerste keer dat de laptop wordt opgestart ziet het login scherm eruitzoals hierboven.

Klik op *Login* om in te loggen.

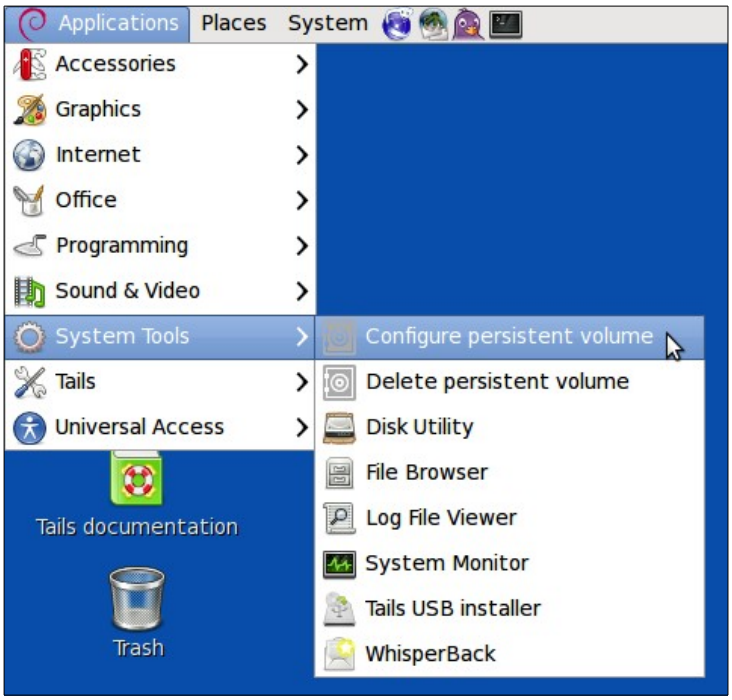
N.B. Nadat een persistent volume is aangemaakt (zie volgende stap), ziet het login scherm eruit zoals hieronder.



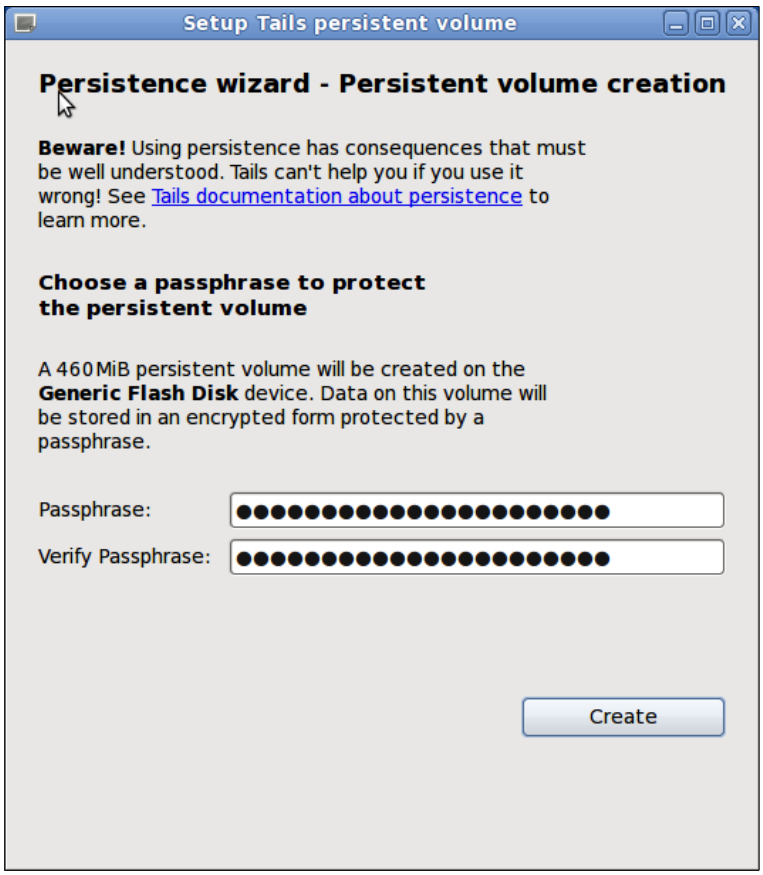
Klik onder *Use persistence?* op *Yes* en voer daarna het wachtwoord van de persistent volume in.

Klik daarna op *Login* om in te loggen.

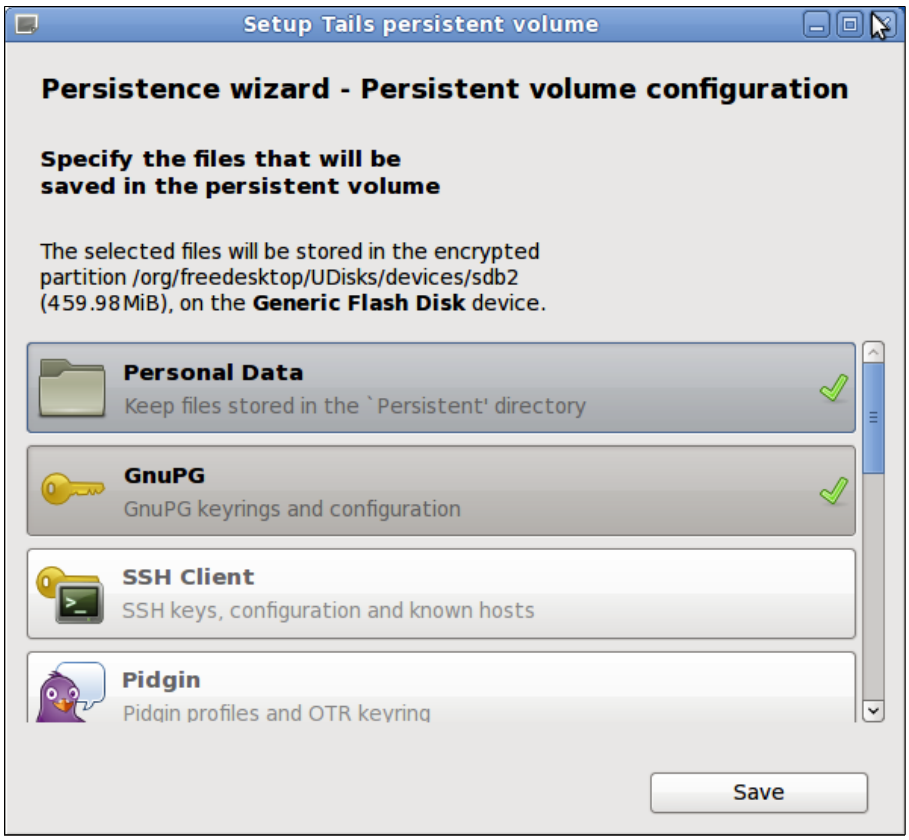
Maak een persistent volume aan



Start *Configure persistent volume*



Voer tweemaal een goede wachtzin in en klik op *Create*



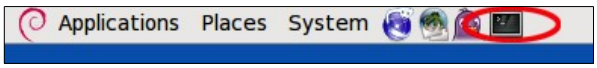
Selecteer de volgende onderdelen:

- Personal Data
- GnuPG
- GNOME Keyring
- Network Connections
- Browser bookmarks

en klik daarna op *Save*.

Sluit vervolgens dit programma af door op het kruisje te klikken en start de laptop opnieuw op.

Het aanmaken van een PGP sleutelpaar



Start een terminal via het icoontje in de bovenste balk.

```
amnesia@amnesia:~ gpg —-gen-key
```

Typ in *gpg --gen-key*, gevolgd door *Enter*.

```
gpg (GnuPG) 1.4.12; Copyright (C) 2012 Free Software Foundation, Inc.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

Please select what kind of key you want:
   (1) RSA and RSA (default)
   (2) DSA and Elgamal
   (3) DSA (sign only)
   (4) RSA (sign only)
Your selection? 1
```

Voer *1* in voor de default optie, gevolgd door *Enter*.

```
RSA keys may be between 1024 and 4096 bits long.
What keysize do you want? (2048) 4096
```

Voer als keysize ***4096***, gevolgd door *Enter*, dat is veiliger dan de default waarde.

```
Requested keysize is 4096 bits
Please specify how long the key should be valid.
         0 = key does not expire
      <n>  = key expires in n days
      <n>w = key expires in n weeks
      <n>m = key expires in n months
      <n>y = key expires in n years
```

```
Key is valid for? (0) 1y
```

Kies voor een geldigheid van één jaar door ***1y*** in te voeren, gevolgd door *Enter*.

```
Key expires at Fri 29 Aug 2014 04:59:08 PM CEST
Is this correct? (y/N) y
```

Type ***y,*** gevolgd door *Enter*.

```
You need a user ID to identify your key; the software constructs the user
ID
from the Real Name, Comment and Email Address in this form:
    "Heinrich Heine (Der Dichter) <heinrichh@duesseldorf.de>"

Real name: Piet Hein (Journalist ABC-MEDIA)
Email address: piet@abc-media.nl
Comment:
You selected this USER-ID:
 "Piet Hein (Journalist ABC-MEDIA) <piet@abc-media.nl>"
```

Voer de naam van je medium in en het e-mail adres dat je voor publeaks gaat gebruiken, het veld *Comment* is optioneel.

```
Change (N)ame, (C)omment, (E)mail or (O)kay/(Q)uit? o
```

Kies *Okay* door ***o*** in te voeren, gevolgd door *Enter*.

```
You need a Passphrase to protect your secret key.
Enter passphrase:
```

Voer een veilig wachtwoord, gevolgd door *Enter*.

```
Repeat passphrase:
```

Herhaal het veilige wachtwoord, gevolgd door *Enter*.

```
We need to generate a lot of random bytes. It is a good idea to perform
some other action (type on the keyboard, move the mouse, utilize the
disks) during the prime generation; this gives the random number
generator a better chance to gain enough entropy.
```

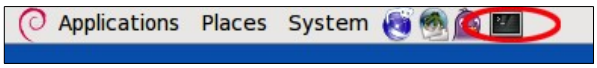
Even geduld, a.u.b.

```
gpg: key ACEB5753 marked as ultimately trusted
public and secret key created and signed.

gpg: checking the trustdb
gpg: 3 marginal(s) needed, 1 complete(s) needed, PGP trust model
gpg: depth: 0  valid:  13  signed:   2  trust: 0-, 0q, 0n, 0m, 0f, 13u
gpg: depth: 1  valid:   2  signed:   0  trust: 1-, 0q, 0n, 0m, 1f, 0u
gpg: next trustdb check due at 2013-12-28
pub   4096R/ACEB5753 2013-08-29 [expires: 2014-08-29]
      Key fingerprint = 8C38 3D1E EBCF 5D1E 6920  14C8 5BDD 5EBE ACEB 5753
uid                  Piet Hein (Journalist ABC-MEDIA) <piet@abc-media.nl>
sub   4096R/04A0F778 2013-08-29 [expires: 2014-08-29]
```

Het aangemaakte sleutelpaar is opgeslagen in de 'keyring' die op de persistent volume is opgeslagen.

Het publieke deel van de PGP key in publeaks zetten



Start de terminal weer.

```
amnesia@amnesia:~ gpg —-export -a piet@abc-media.nl
```

Typ in ***gpg --export -a <e-mail adres>*** waarbij <e-mail adres> het e-mail adres is dat je tijden het maken van de PGP key hebt gebruikt (in ons voorbeeld piet@abc-media.nl).

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v1.4.11 (GNU/Linux)

mQENBFG+/FABCAC6DrMMOEhWMopDNqyV7w/SGdUwHwbXEQ60ftIX5Zbp27HHf7bk
[...]
FJrI4kaRN/b40sDI24nN5v20VLvm+RDkzPq3TliT9f9TBrh/R48mjBw4ksfbmYVf
-----END PGP PUBLIC KEY BLOCK-----
```

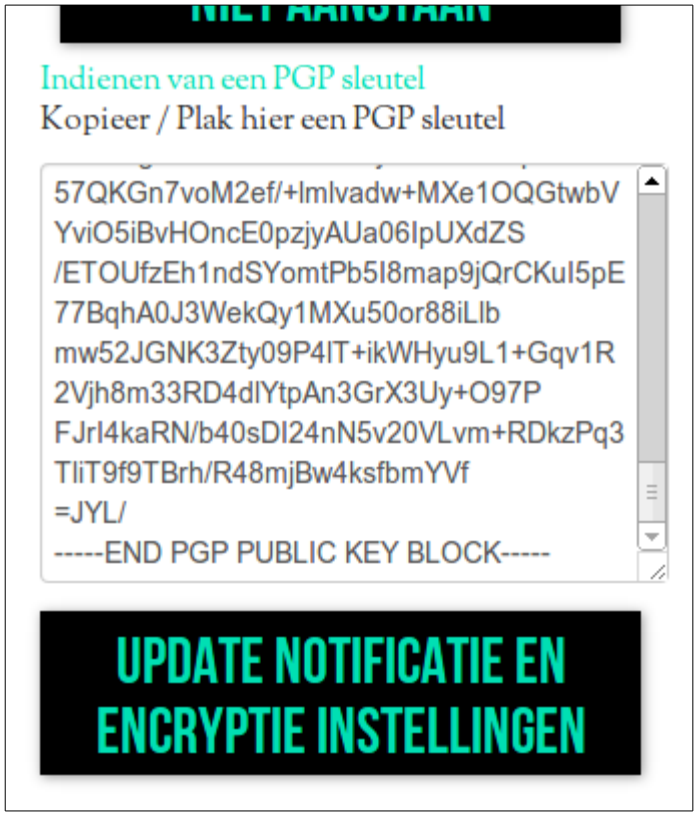
Kopieer de hele tekst die op het scherm verschijnt, van `-----BEGIN PGP PUBLIC KEY BLOCK-----` tot en met `-----END PGP PUBLIC KEY BLOCK-----`

Start op de laptop de browser en ga naar https://secure.publeaks.nl

Log in door te klikken op *Login pagina* en je gebruikersnaam en wachtwoord in te voeren.

Klik op *Voorkeuren* en scroll naar beneden naar de *Encryption settings*.

Klik indien nodig op *Indienen van een PGP sleutel* om het PGP veld te openen.



Plak de eerder gekopieerde public PGP key in het veld.

N.B. Als het veld reeds een PGP key bevat, verwijder deze dan eerst voor de eigen key te plakken.

Klik daarna op *UPDATE NOTIFICATIE EN ENCRYPTIE INSTELLINGEN*.

Ophalen van een tip

Start op de laptop de browser en ga naar https://secure.publeaks.nl

Log in door te klikken op *Login pagina* en je gebruikersnaam en wachtwoord in te voeren.

Nadat je bent ingelogd toont de website de verschillende tips die je hebt ontvangen.

Klik op het getal dat onder *Toegang* staat om de desbetreffende tip te bekijken.

Uitleg van de verschillende kolommen:

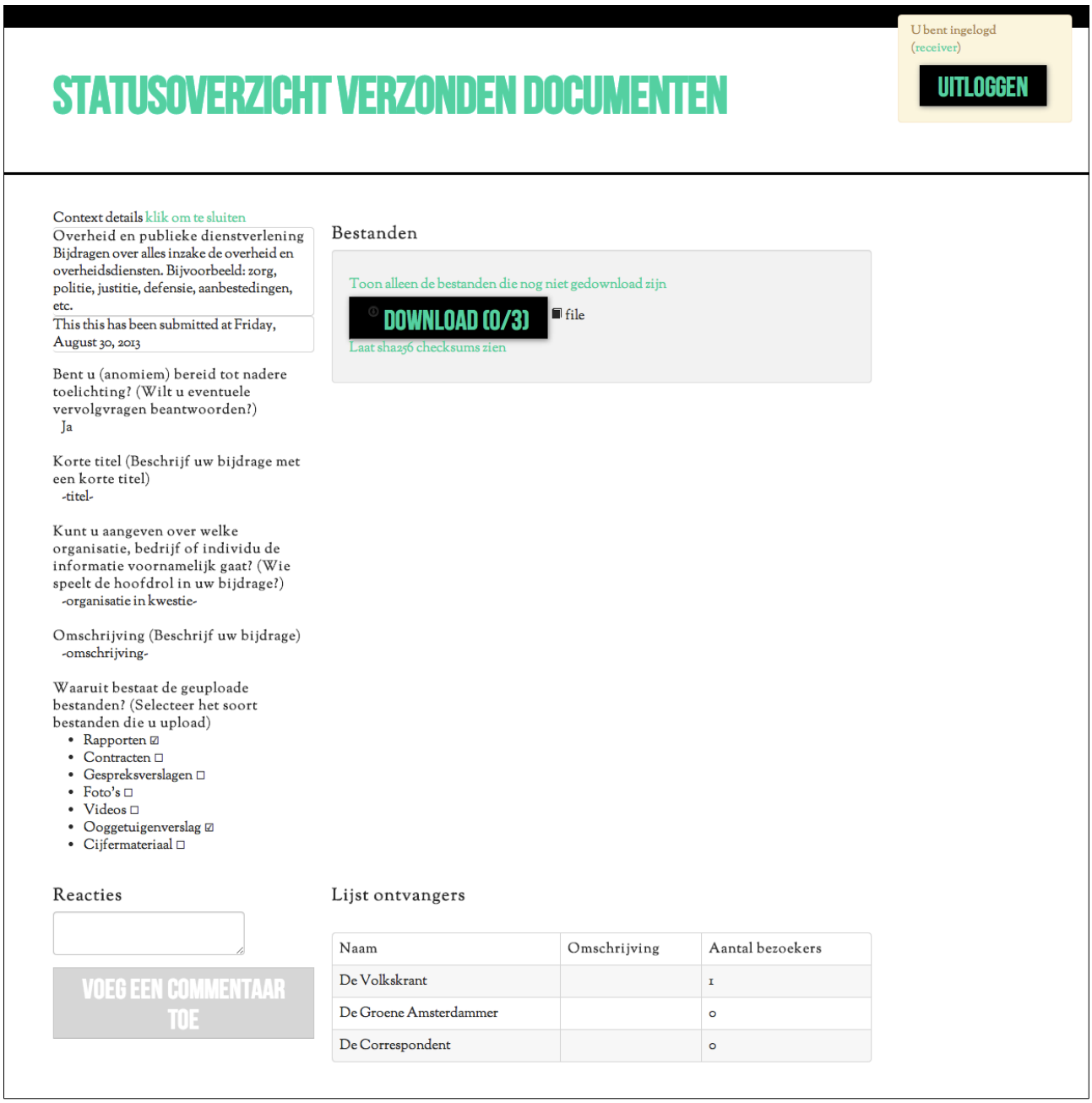
Toegang: Het aantal maal dat je deze tip hebt bekeken.

Schepping: De datum waarop de tip is ingediend.

Laatste bezoek: De datum waarop je de tip voor het laatst hebt bekeken.

Voorbeeld: (wordt nog verwijderd)

Bestanden: Het aantal bestanden dat in de tip is geüpload.



Op de statusoverzicht pagina staat alle relevant informatie over de ingezonden tip:

Context details: Alle informatie die de tipgever over de tip heeft meegestuurd.

Bestanden: De bestanden die de tipgever heeft meegestuurd en hoe vaak ze zijn gedownload.

N.B. Je kunt de bestanden maximaal 3 keer downloaden.

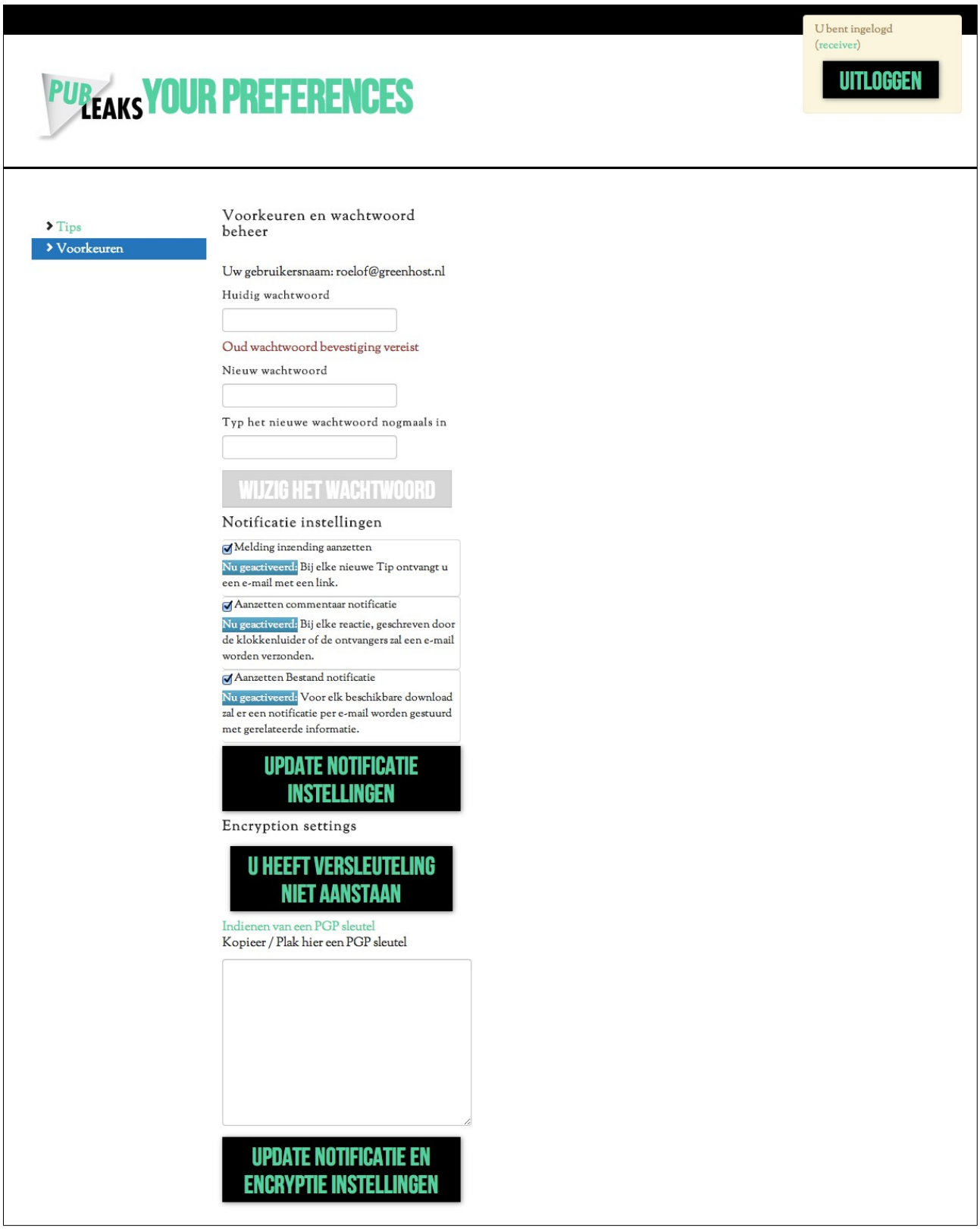
Reacties: Een lijst van reacties van zowel de journalist als van de tipgever.

Een reactie geven kan door in het lege veld te schrijven en te klikken op Voeg een commentaar toe.

N.B. De tipgever krijgt geen meldingen, hij moet zelf kijken of er (nieuwe) berichten zijn.

N.B. Niet alleen de tipgever, maar ook de andere ontvangers kunnen deze reacties lezen.

Lijst ontvangers: Een overzicht van welke media deze tip hebben ontvangen en hoe vaak die desbetreffende media de tip hebben bekeken.



Op de *Voorkeuren* zijn een aantal dingen in te stellen :

Uiteraard kun je je wachtwoord wijzigen. N.B. Maak alleen gebruik van een sterk wachtwoord!

Je kunt instellen dat meldingen je wilt ontvangen als een tipgever een tip upload of een tipgever de ingestuurde tip wijzigt.

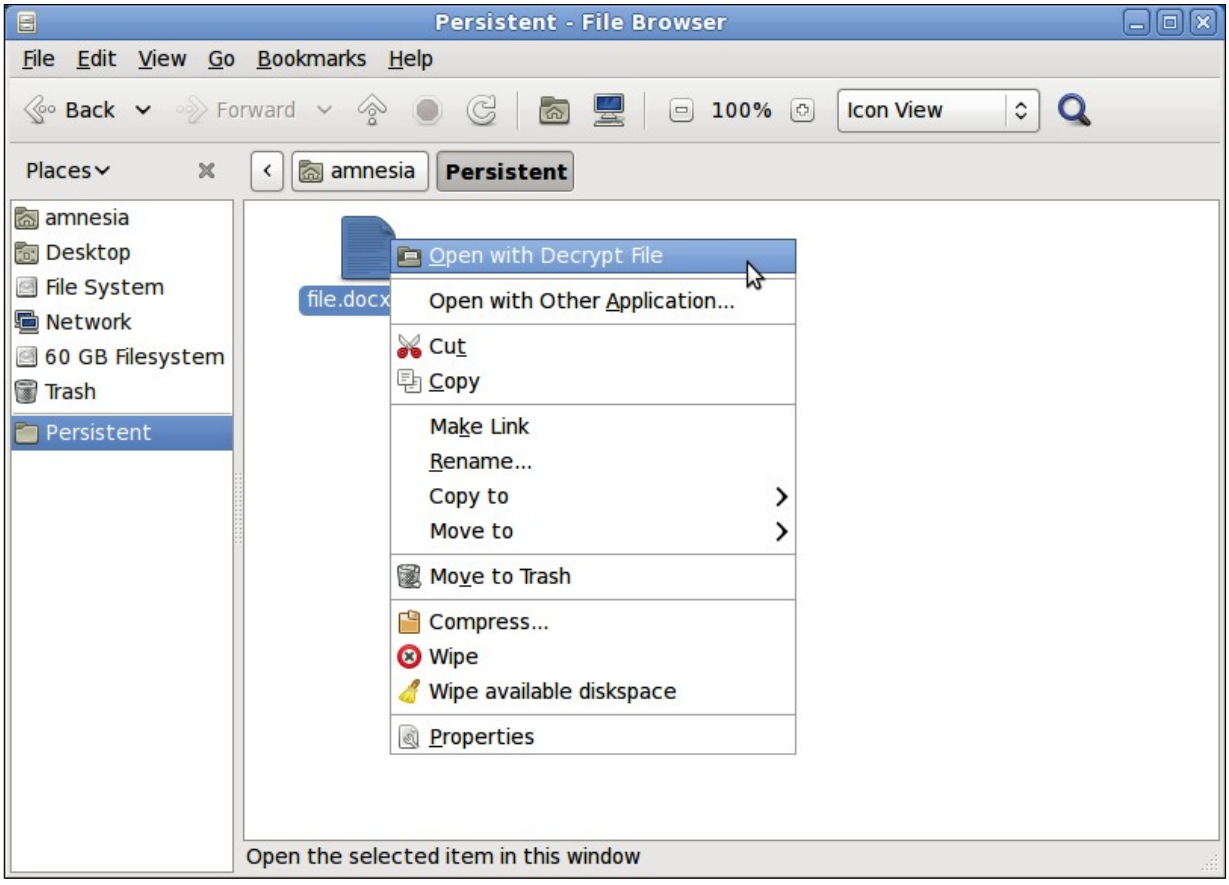
Je kunt hier het publieke deel van je PGP key invoeren, daarmee worden de ingediende bestanden dan versleuteld.

Decrypten van een toegezonden bestand

Download het bestand dat je wilt decrypten en sla dit op je laptop op in de map *Persistant*.

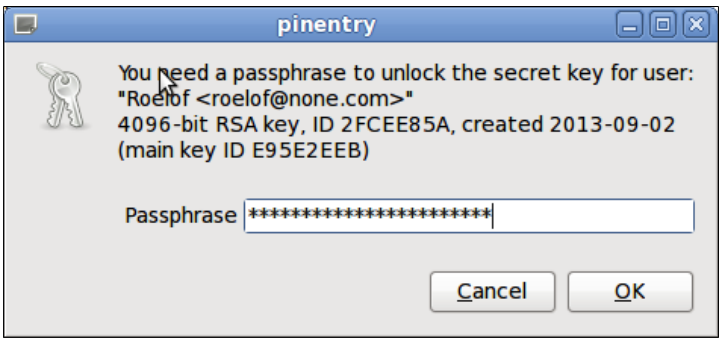
N.B. Bestanden die niet in de map *Persistant* worden opgeslagen verdwijnen als de laptop wordt herstart.

Open de filebrowser, bijvoorbeeld door op de map *amnesia* op de desktop te klikken.

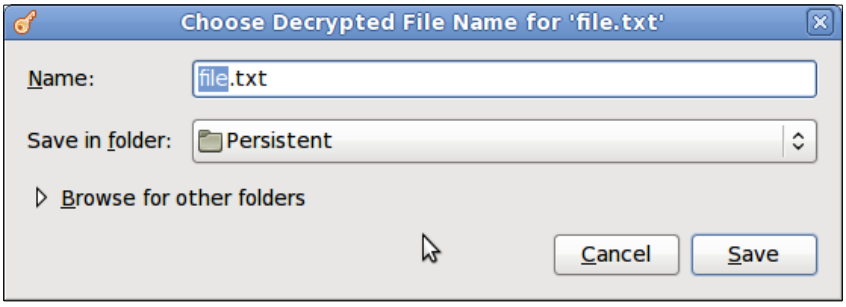


Rechtermuisklik op het bestand dat je wilt decrypten.

N.B. De bestanden die encrypt zijn met PGP hebben meestal de extensie .pgp, maar dat hoeft niet het geval te zijn.



Voer het wacthwoord van je PGP-key in en klik op *OK*.



Kies de locatie waar je het gedecrypte bestand op wilt slaan.

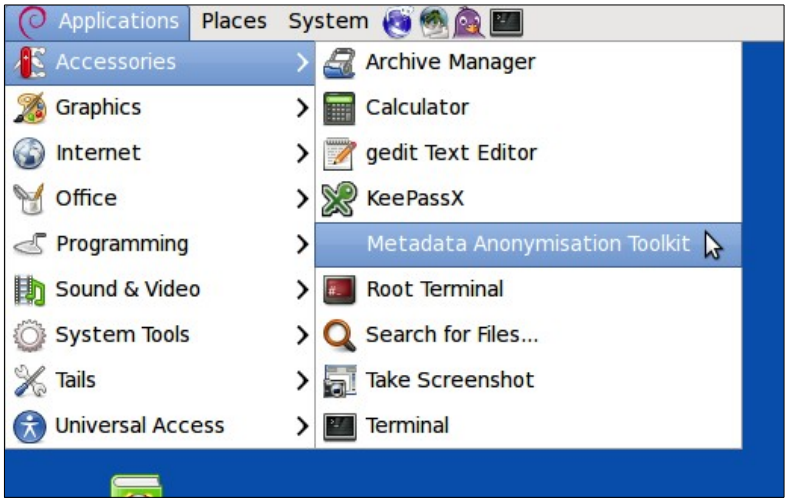
Metadata verwijderen van bestanden

In bestanden staat vaak metadata over de gebruiker die het bestand heeft gemaakt of bewerkt. Deze gegevens zouden mogelijkheid de identiteit van de tipgever kunnen verraden. Daarom is het verstandig om de metadata van bestanden eerst te verwijderen voordat ze elders, buiten deze versleutelde laptops, worden gebruikt.

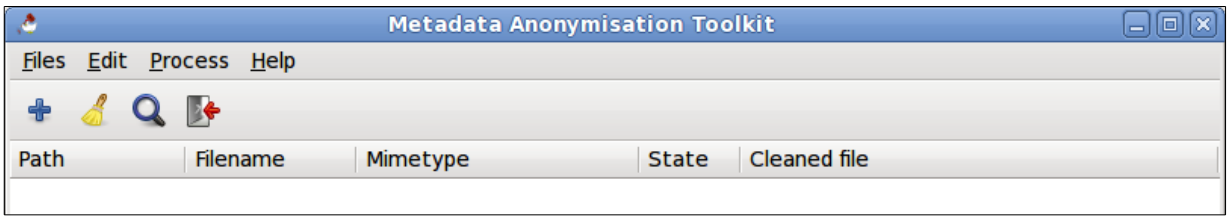
N.B. Dat een bestand geen metadata meer bevat, betekend natuurlijk niet dat de inhoud van het bestand niet alsnog de identiteit van de tipgever kan verraden.

Het verwijderen van deze metadata kan met het programma *Metadata Anonymisation Toolkit*. Dit programma is geschikt voor een heel aantal bestandssoorten, maar niet alle. Eén van de bestandssoorten die het programma helaas niet kan bewerken zijn .doc bestanden (wel .docx). Indien .doc bestanden aanwezig zijn kunnen deze met behulp van OpenOffice worden omgezet naar .odt bestanden en die kunnen wel worden bewerkt.

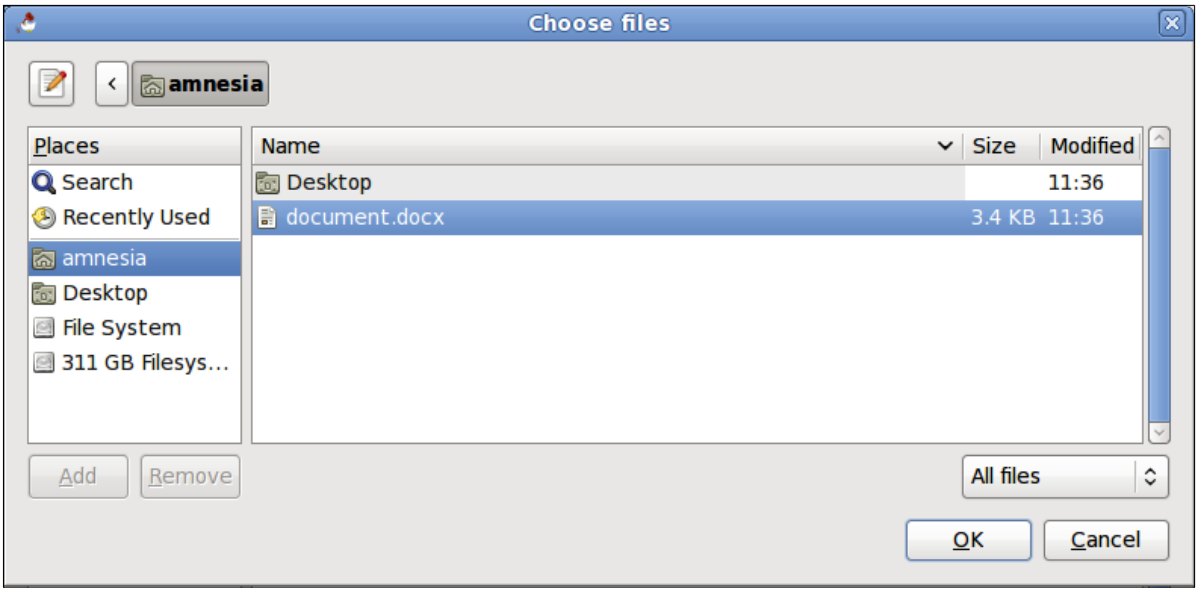
Hieronder een korte handleiding voor het gebruik van *Metadata Anonymisation Toolkit*:



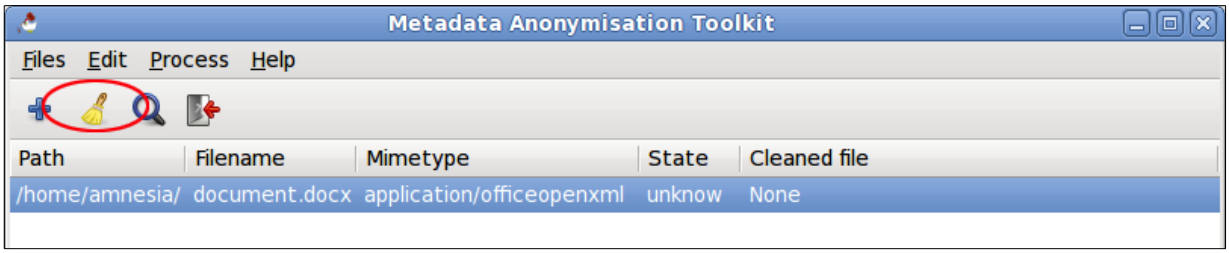
Start de applicatie via *Applications* > *Accessories* >*Metadata Anonymisation Toolkit*



Klik op het plusteken om een bestand toe te voegen.

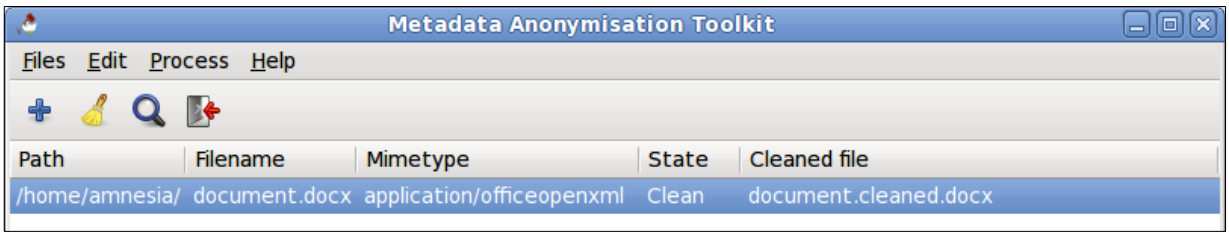


Selecteer een of meerdere bestanden en klik op *OK*.



Selecteer een of meerdere bestanden en klik op 'de bezem' of start via *Process* en dan *Clean*

De *state* geeft aan of een bestand metadata bevat (D*irty*) of niet (C*lean*), of dat het onbekend is en nog moet worden onderzocht (*unknown*).



Vervolgens is in het programma te zien dat het bestand is ontdaan van de metadata (Clean) en is opgeslagen als <naam>.cleaned.<extensie>.

Het bestand wordt standaard in dezelfde map opgeslagen als het originele bestand.

Backups

Zoals bij alle techniek is ook bij Publeaks niet uit te sluiten dat er een keer een defect in de apparatuur op zal treden. Daarom is het altijd verstandig om backups te maken. Voor de servers doen wij dit uiteraard, maar maar voor de laptops ligt die verantwoordelijkheid bij de journalist.

Het belangrijkste waar een backup van moet worden gemaakt, is de PGP sleutel op de usb-stick. Als deze sleutel namelijk verloren gaat, dan wordt de versleutelde data volledig ontoegankelijk.

Of het ook nodig is om een backup te maken van de rest van de data die op de usb-stick staat, dat is aan de journalist om te beoordelen.

N.B. Wees voorzichtig met het maken van backups van gevoelige data!

Alle data die op de usb-stick staat is veilig opgeslagen in een versleuteld volume. Als er een backup wordt gemaakt, dan is het mogelijk dat deze op een onversleutelde plek wordt opgeslagen.
Voor de PGP sleutel is dit niet zo erg, die is beveiligd met een lang en goed wachtwoord. Alle andere data op de usb-stick heeft deze extra beveiliging niet, die wordt alleen beschermd door het versleutelde volume. Het is daarom verstandig om zeer voorzichtig te zijn bij het maken van een backup van gevoelige data.

Backup maken van de PGP sleutel

Alle data van de persistent volume staat in een map op de usb stick. De inhoud van deze map kan makkelijk als backup worden gekopiëeerd. Hieronder is te lezen waar deze data precies staat.

Klik op *Computer* die op de desktop staat. Klik vervolgens op *File System*, op *live*, op *persistence* en op *sdb2_unlocked*. In deze laatste map staan alle de bestanden die in de persitent volume staan.

De map *gnupg* bevat alle PGP sleutels die op het systeem staan. Het volstaat om deze hele map te naar een veilige plek buiten de laptop en de usb-stick te kopieëren. (Eventueel kan een tweede usb-stick worden gebruikt voor het transport van de laptop naar een andere computer.)

Een andere manier om de PGP sleutel te kopieëren, is door een export te maken en deze op te slaan.

Met het commando *gpg --export-secret-keys -a <e-mail adres>* kan de privé sleutel worden geëxporteerd zoals we eerder ook de publieke sleutel hebben geëxporteerd. Deze export kan als een tekst bestand op een veilige plek als backup worden opgeslagen.

Updaten van Tails

Zoals bij elk systeem worden ook voor Tails met enige regelmaat nieuwe versies gemaakt. Deze nieuwe versies kunnen verbeteringen en uitbreidingen bevatten, maar belangrijker is dat ze mogelijk ook beveiligingsproblemen oplossen. Het is dus belangrijk om zoveel mogelijk de laatste versie van Tails te gebruiken.

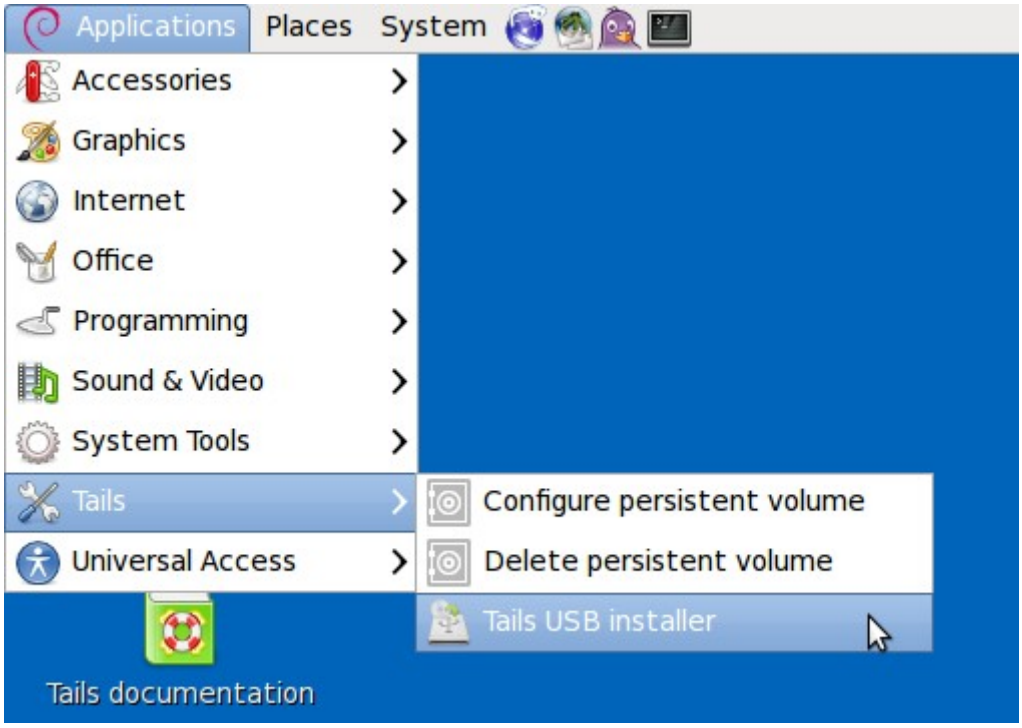
Belangrijk bij het updaten is natuurlijk dat aanwezige data in de persistent volume niet verloren gaat. Bij het updaten zoals dat hier beneden is beschreven blijft de persitent volume gewoon in tact, maar een backup maken voor een update is nooit onverstandig.

De Tails usb-stick kan alleen worden geüpdate vanaf een ander Tails usb-stick (of cd) waar wél de laatste versie op staat.

Creëeer dus allereerst een nieuwe Tails usb-stick met de laatste versie. Deze laatste versie is te downloaden op https://tails.boum.org. Een handleiding over het maken van de usb-stick is te vinden op https://tails.boum.org/doc/first_steps/manual_usb_installation/index.en.html

Start de laptop op met de net gemaakte Tails usb-stick en log in.

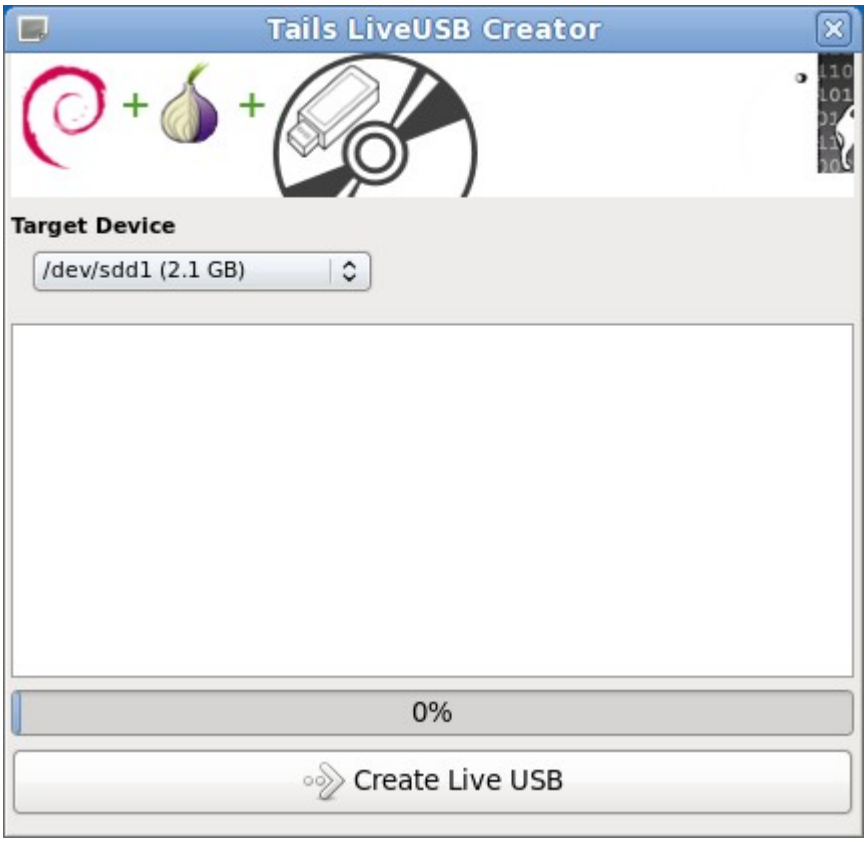
N.B. De usb-stick die je wilt updaten mag niet in de laptop zitten.



Start de *Tails USB installer*

Klik op *Clone & Upgrade*

Steek de Tails usb-stick die je wilt upgraden in de laptop.



Klik op *Create Live USB* en klik op *Next*.

Het updaten duurt even en daarna kan op *OK* worden geklikt om het programma te sluiten.

De Tails usb-stick is nu geüpdate en kan weer worden gebruikt.