FreieSoftwareOG –

Kurz Hand-Ons IV - kleine Tools schnell vorgestellt

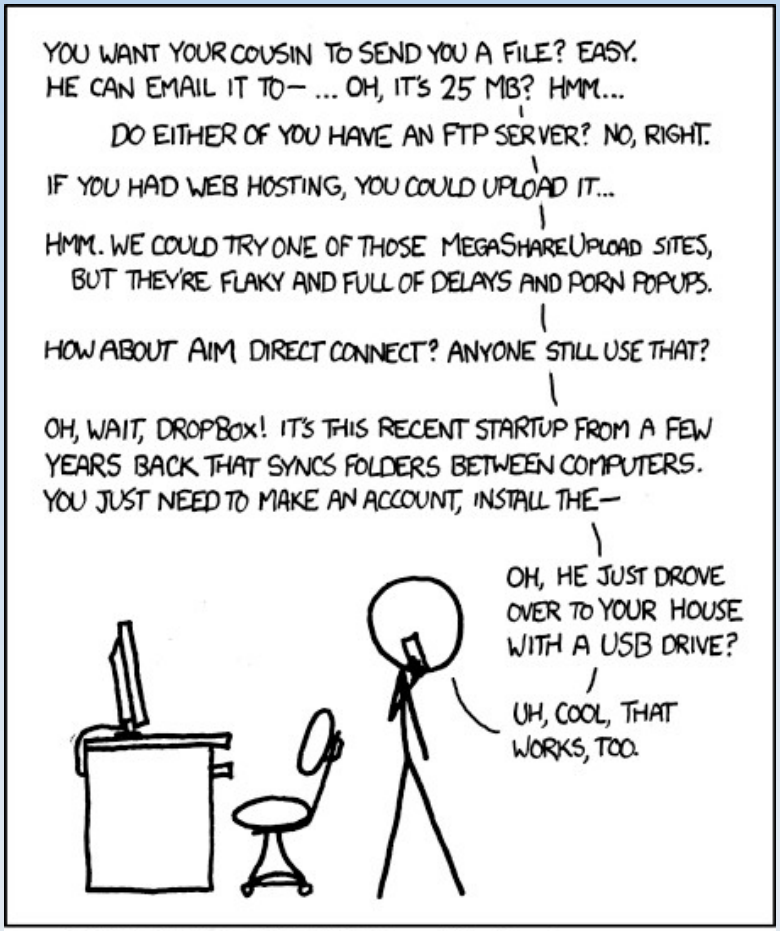
Hands-Ons – Was soll das sein?

In dieser Serie werden wir jeweils 2 bis 3 kleine Tools und/oder Methoden kennenlernen und diese auch direkt ausprobieren.

Hands-On 1 – Einfacher HTTP-Server

Das Werkzeug:	weborf
Die Alternative(n):	Apache, …
Das Thema:	Webserver (konfigurationslos)
Die Aufgabe(n):	Einfaches Zugänglichmachen von Dateien über das Web

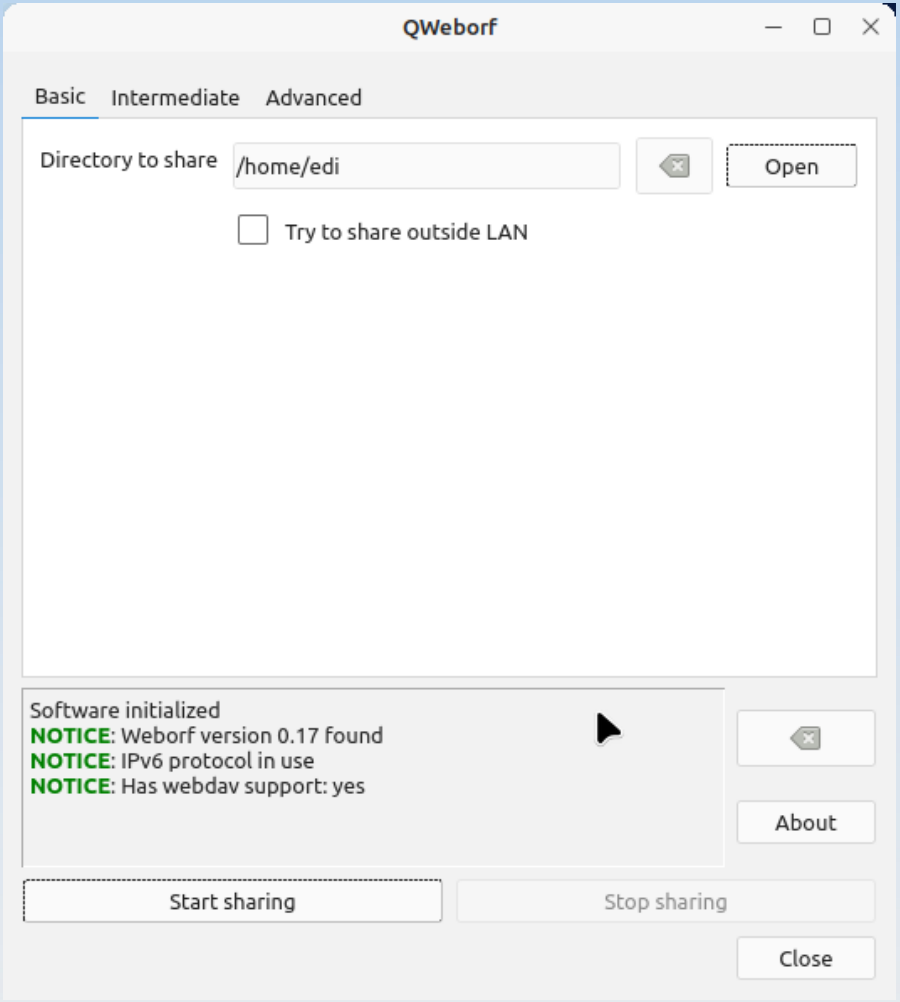
Hands-On 1 – weborf



I LIKE HOW WE'VE HAD THE INTERNET FOR DECADES, YET "SENDING FILES" IS SOMETHING EARLY ADOPTERS ARE STILL FIGURING OUT HOW TO DO.

FreieSoftwareOG.org

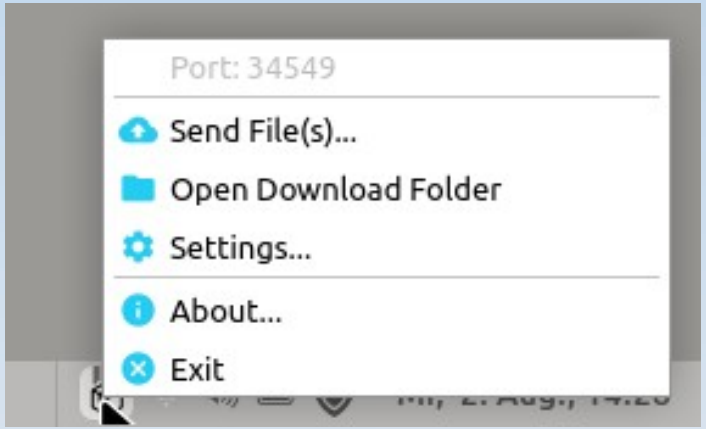
Hands-On 1 – weborf/qweborf

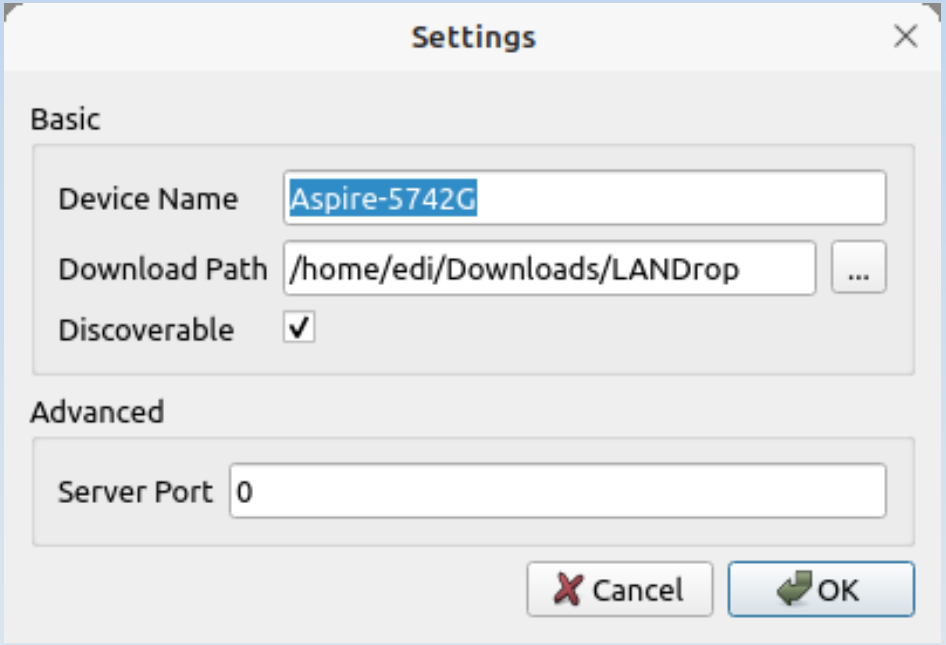


Hands-On 2 – Ad Hoc File sharing

Das Werkzeug:	LANDrop
Die Alternative(n):	xxx
Das Thema:	Dateien schnell und unkompliziert teilen
Die Aufgabe(n):	Dateien schnell und unkompliziert und sicher teilen

Hands-On 2 - LANDrop



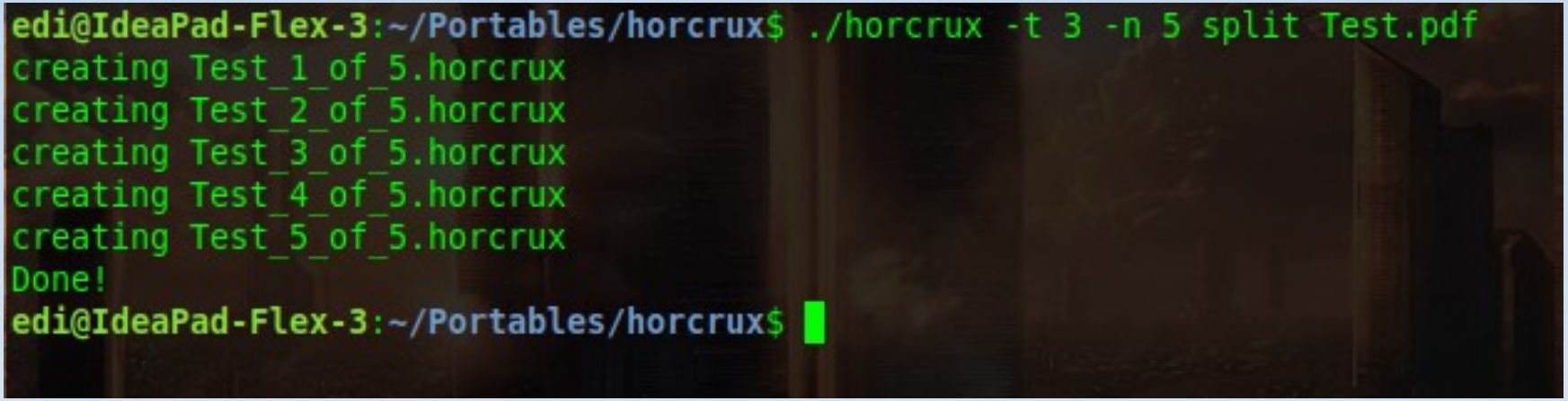


FreieSoftwareOG.org

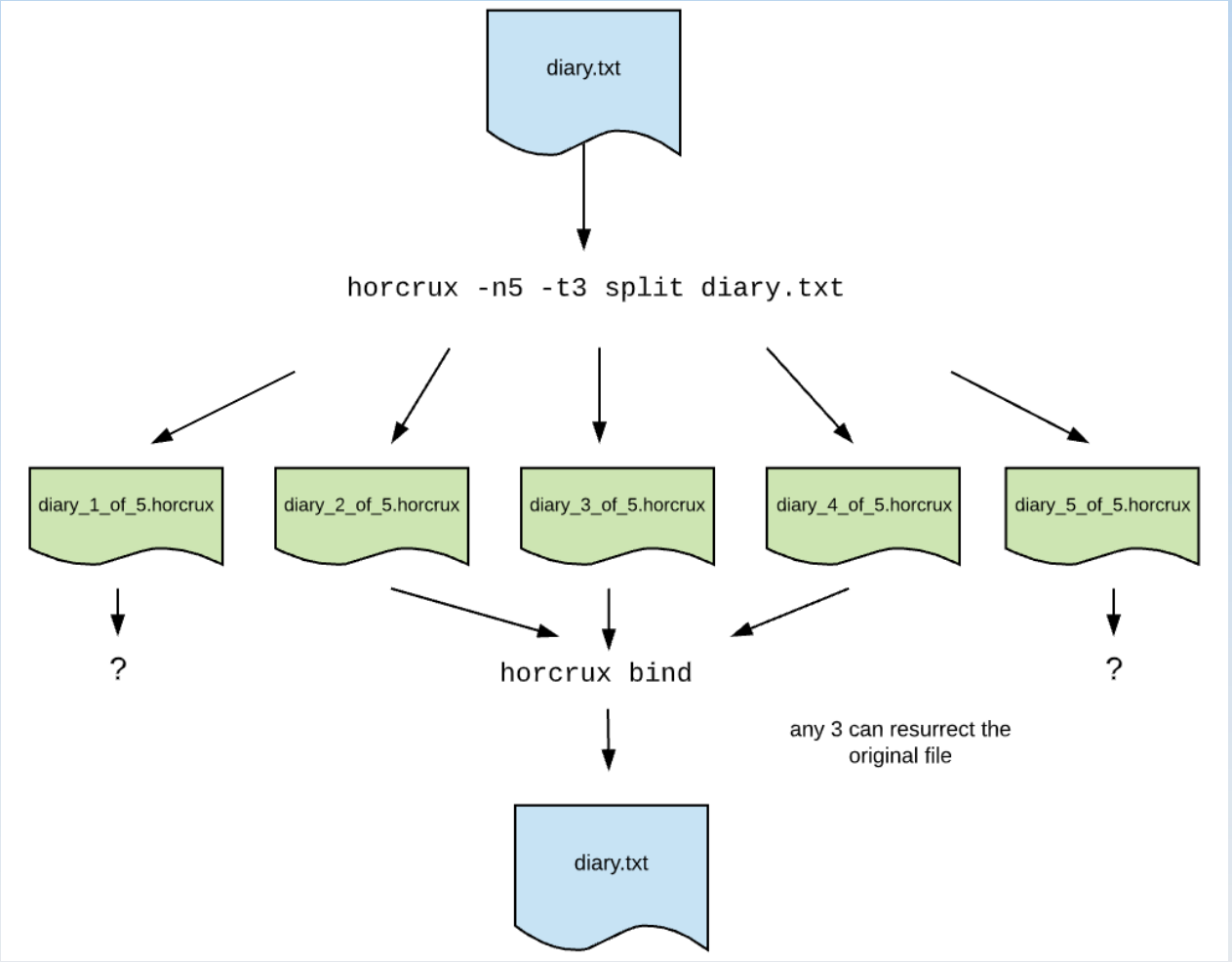
Hands-On 3 – Dateien sicher aufteilen

Das Werkzeug:	horcrux
Die Alternative(n):	haystack, ssss
Das Thema:	Große Dateien zerstückeln
Die Aufgabe(n):	Eine Datei in verschiedene Teile teilen

Hands-On 3 – horcrux



Hands-On 3 – horcrux



Hands-On 3 – horcrux

Shamir's Secret Sharing

Shamir's Secret Sharing ist ein 1979 von Adi Shamir entwickeltes Secret-Sharing-Verfahren. Mit Hilfe eines solchen Verfahrens kann man ein Geheimnis so auf mehrere „Instanzen" (Mitwisser) au
sämtliche Instanzen benötigt werden).

Inhaltsverzeichnis [Verbergen]

Idee des Verfahrens [Quelltext bearbeiten]

Der „Dealer" (benannt nach dem Kartengeber bei einem Kartenspiel) bestimmt eine Zahl t an Instanzen, die das Geheimnis später wieder rekonstruieren können sollen und wählt daraufhin ein Polyr
Instanzen können daraufhin mit einem Interpolationsverfahren das Polynom rekonstruieren, dessen konstanter Term das Geheimnis ist.

Ablauf [Quelltext bearbeiten]

Der Dealer wählt ein Polynom

$$f(x) = s + a_1 \cdot x + a_2 \cdot x^2 + \cdots + a_{t-1} \cdot x^{t-1}$$

wobei s das Geheimnis ist und die a_i zufällig gewählt werden. Nun erzeugt der Dealer n Wertepaare $(x_i, s_i = f(x_i))$, wobei $x_i \neq 0$ und verteilt diese Wertepaare an die beteiligten Instanzen. Die

Nach dem Fundamentalsatz der Algebra benötigt man t Wertepaare $(x, f(x))$, um dieses Polynom eindeutig zu bestimmen. Daher können bis zu $t-1$ Shares kompromittiert werden, ohne dass da
Geheimnisses t Instanzen ihre Shares kombinieren müssen, um das Geheimnis zu erhalten.

Dieses System wird auch als (t,n)-Schwellwert-Kryptosystem bezeichnet, da nur t der gesamten n Shares benötigt werden, um das Geheimnis zu rekonstruieren.

Rekonstruktion mittels der Lagrange-Interpolation [Quelltext bearbeiten]

Zur effizienten Rekonstruktion des Polynoms kann die Lagrange-Interpolation benutzt werden.

$$g(x) = \sum s_i \cdot \prod_{j \neq i} \frac{x - x_j}{x_i - x_j}$$

Da das Geheimnisses aber nur konstanten Term s ist, reicht es $g(0)$ zu berechnen

$$s = g(0) = \sum s_i \cdot \prod_{j \neq i} \frac{-x_j}{x_i - x_j}$$

Jeder Teilnehmer berechnet nun

$$w_i = s_i \cdot \prod_{j \neq i} \frac{-x_j}{x_i - x_j}$$

und hat dadurch einen additiven Teil des Geheimnisses $s = \sum w_i$.

LPI - Fragen

LPI - Frage #6

DNS liefert … zu IP-Adressen.

A) NETBIOS Namen
B) Hostnamen
C) MAC-Adressen

Antwort: B

Bitte beachten

Auf der Homepage findet sich immer das

aktuelle Datum, sowie das Thema des nächsten Treffens!

Weitergehende Informationen

http://github.com/ltworf/weborf

https://landrop.app/

https://github.com/jesseduffield/horcrux

https://de.wikipedia.org/wiki/Shamir%E2%80%99s_Secret_Sharing

Weitere Informationen bekommen Sie hier:

http://www.FreieSoftwareOG.org

und

Kontakt@FreieSoftwareOG.org

oder kommen Sie doch einfach zu unserem regelmäßigen Treffen,
jeden 1. Mittwoch im Monat ab 20:00 Uhr.
(Treffpunkt laut Webseite)