

Obfuscation I

Information Privacy with Applications
David Sidi (dsidi@email.arizona.edu)

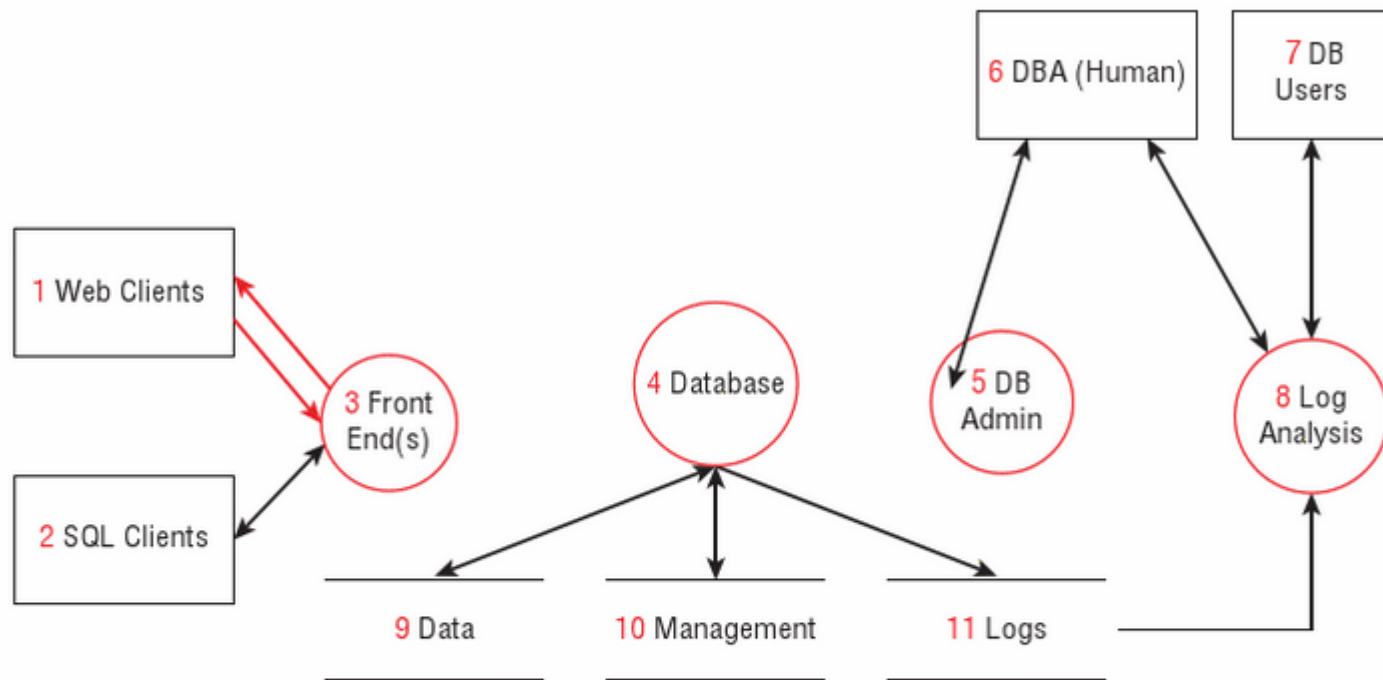
Administration

- Server Assignment II: Cracking
- <https://3rd.obfuscationworkshop.org/reception>

Finishing up last time: Focusing on Software in Threat Modeling

- Point is to diagram how the system works
- Done in a group with a wide variety of people (you want them to turn out to be across trust boundaries): if there is disagreement, this usually means a security problem is nearby

Data flow diagrams



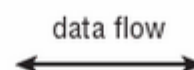
Key:



External Entity



Process



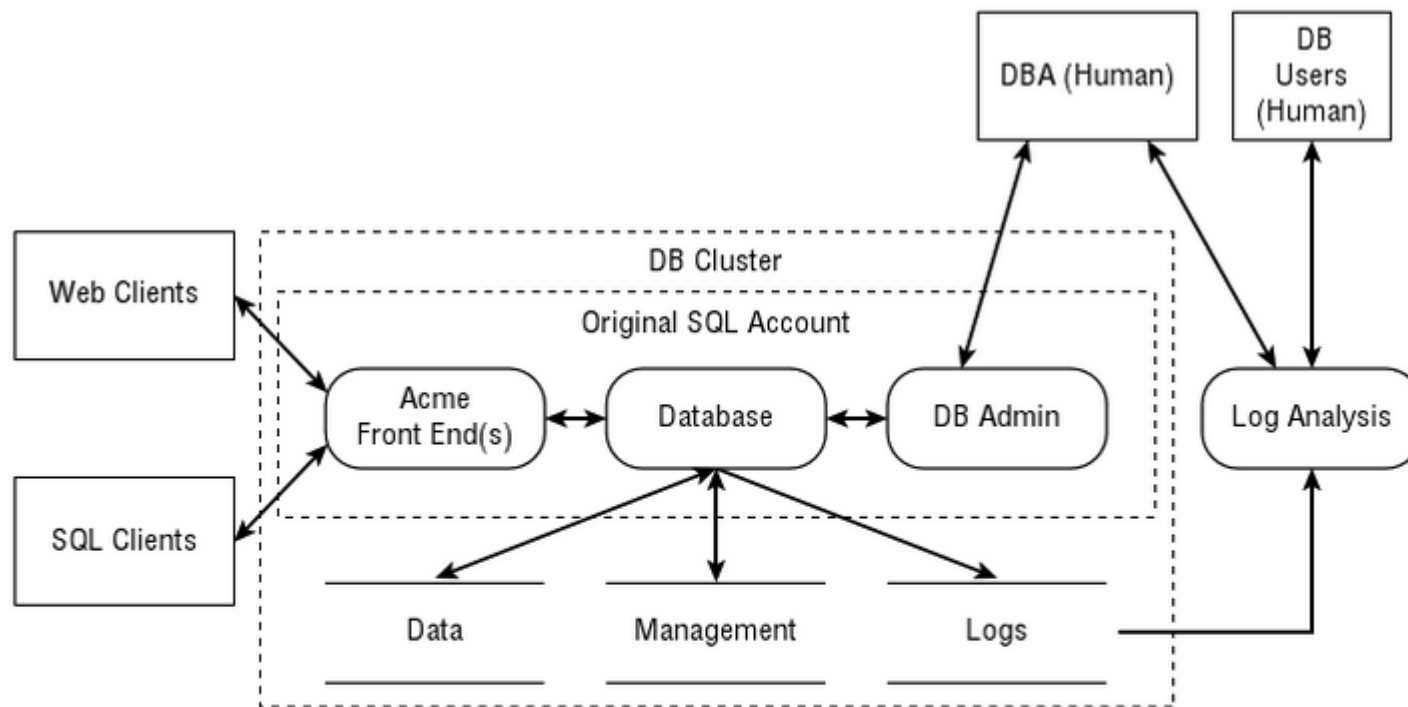
data flow



Data Store

Figure 2-3: A classic DFD model

Data flow diagrams



Key:

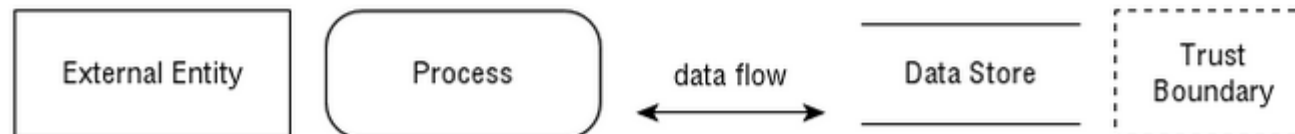


Figure 2-4: A modern DFD model (previously shown as Figure 2-1)

Swim lane diagrams

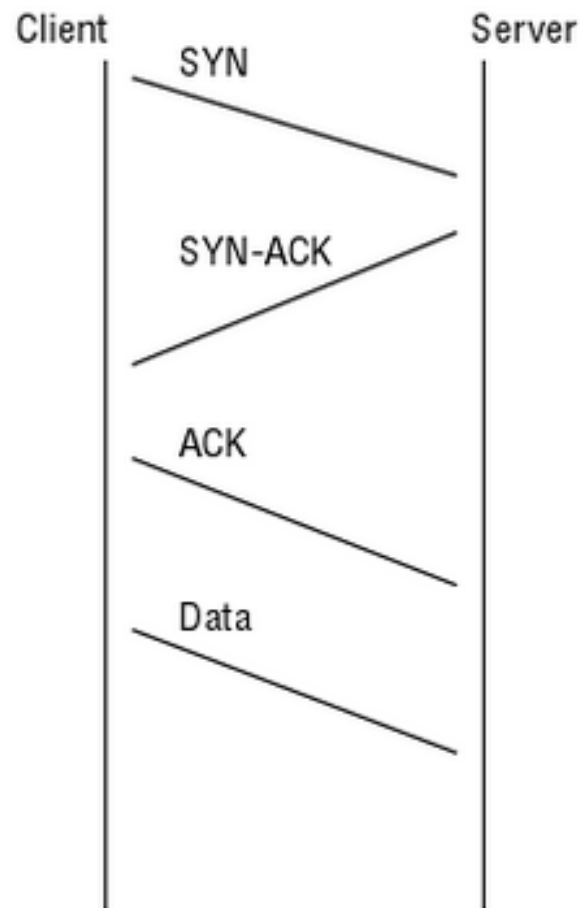
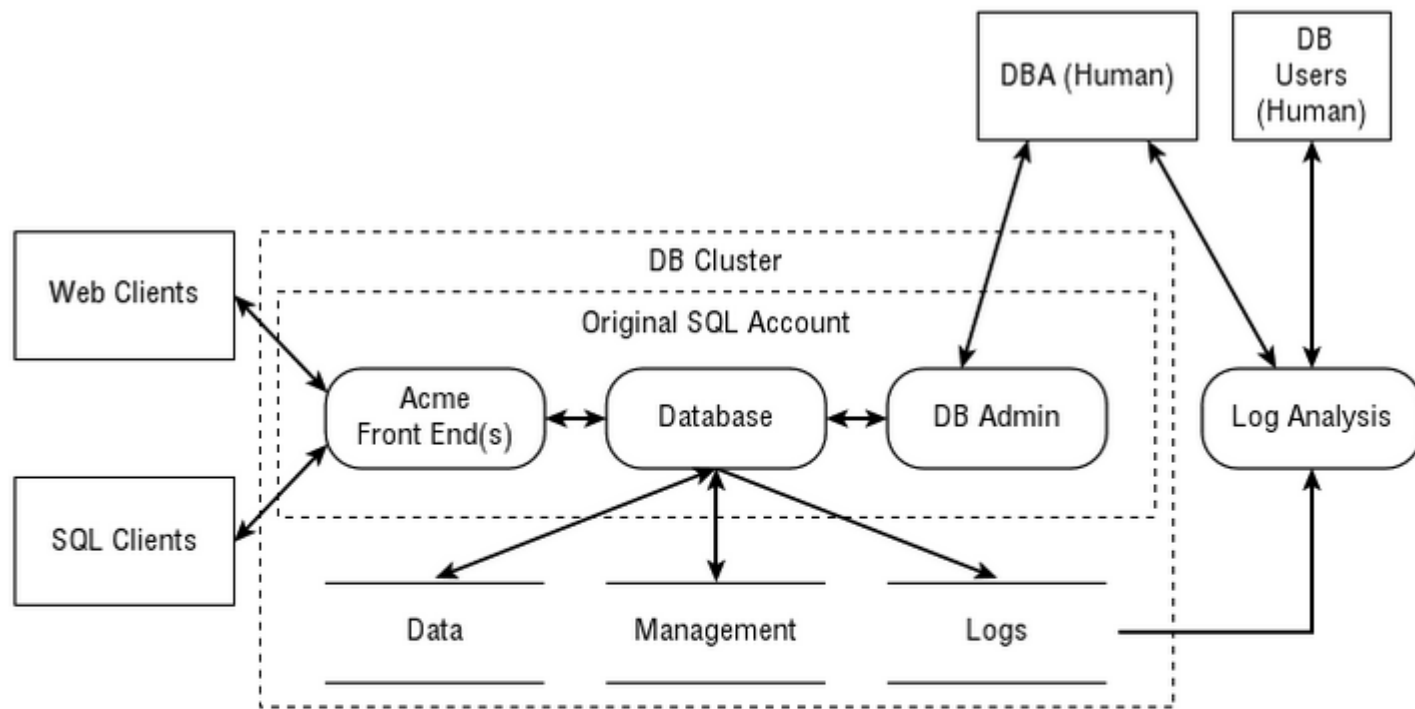


Figure 2-6: Swim lane diagram (showing the start of a TCP connection)

Processing and Managing Threats



Key:

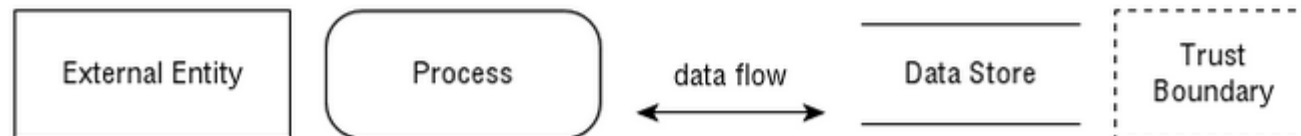
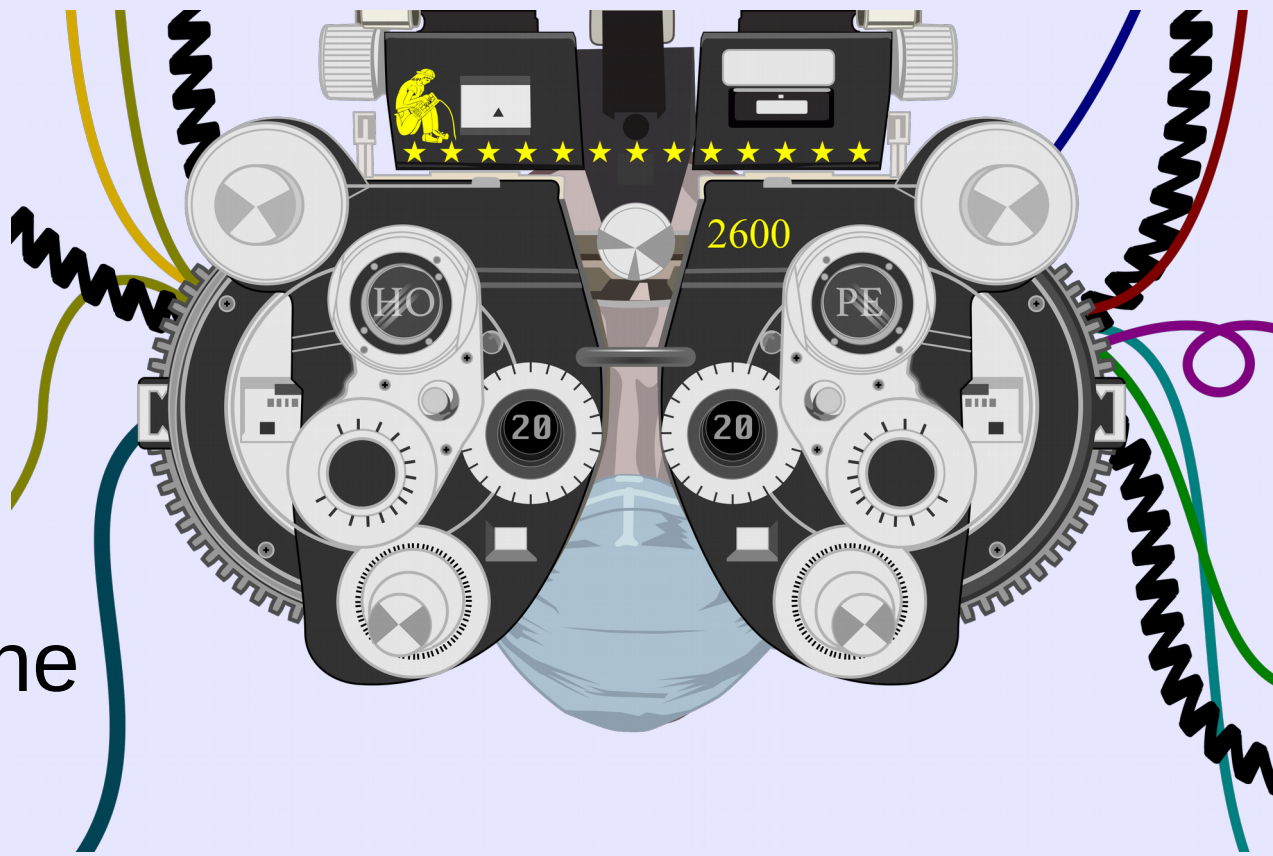


Figure 2-4: A modern DFD model (previously shown as Figure 2-1)

- 2600 meetings near Harvard in the early 1990s, recounted in the cDc book



“Obfuscation, at its most abstract, is the production of noise modeled on an existing signal in order to make a collection of data more ambiguous, confusing, harder to exploit, more difficult to act on, and therefore less valuable.”

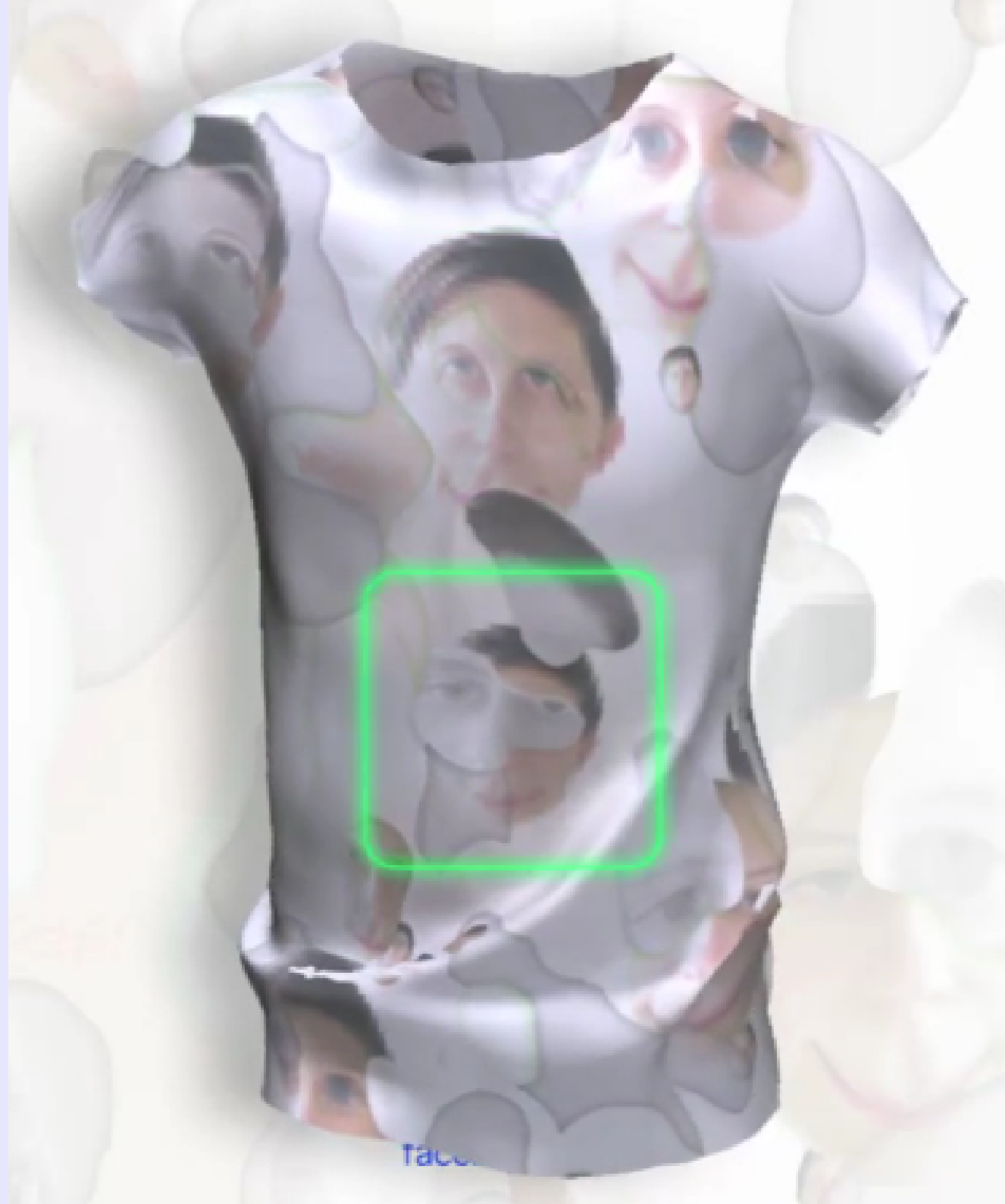
“If privacy both as impossible-to-observe and impossible-to-identify is dead, then what might be an alternative? If you’re an optimist or an apparatchik, your answer will tend toward rules of procedure administered by a government you trust or control. If you’re a pessimist or a hacker/maker, your answer will tend toward the operational, and your definition of a state of privacy will be mine: the effective capacity to misrepresent yourself.”

Geer, ‘Identity as Privacy’



An adult *C. mulmeinensis* alongside decoy prey pellets (L) and decoy egg sacs (R)



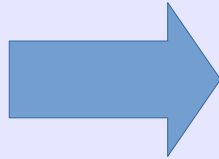


Obfuscation for confidentiality: chaffing and winnowing

Chaffing & Winnowing

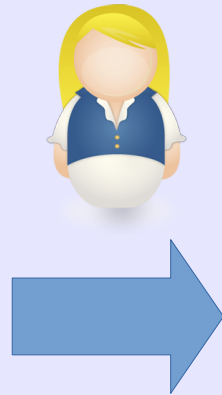


(1,Hi Bob,465231)
(2,Meet me at,782290)
(3,7PM,344287)
(4,Love-Alice,312265)



(1,Hi Larry,532105)
(1,Hi Bob,465231)
(2,Meet me at,782290)
(2,I'll call you at,793122)
(3,6PM,891231)
(3,7PM,344287)
(4,Yours-Susan,553419)
(4,Love-Alice,312265)

(1,Hi Bob,465231)
(2,Meet me at,782290)
(3,7PM,344287)
(4,Love-Alice,312265)



(1,Hi Larry,532105)
(1,Hi Bob,465231)
(2,Meet me at,782290)
(2,I'll call you at,793122)
(3,6PM,891231)
(3,7PM,344287)
(4,Yours-Susan,553419)
(4,Love-Alice,312265)



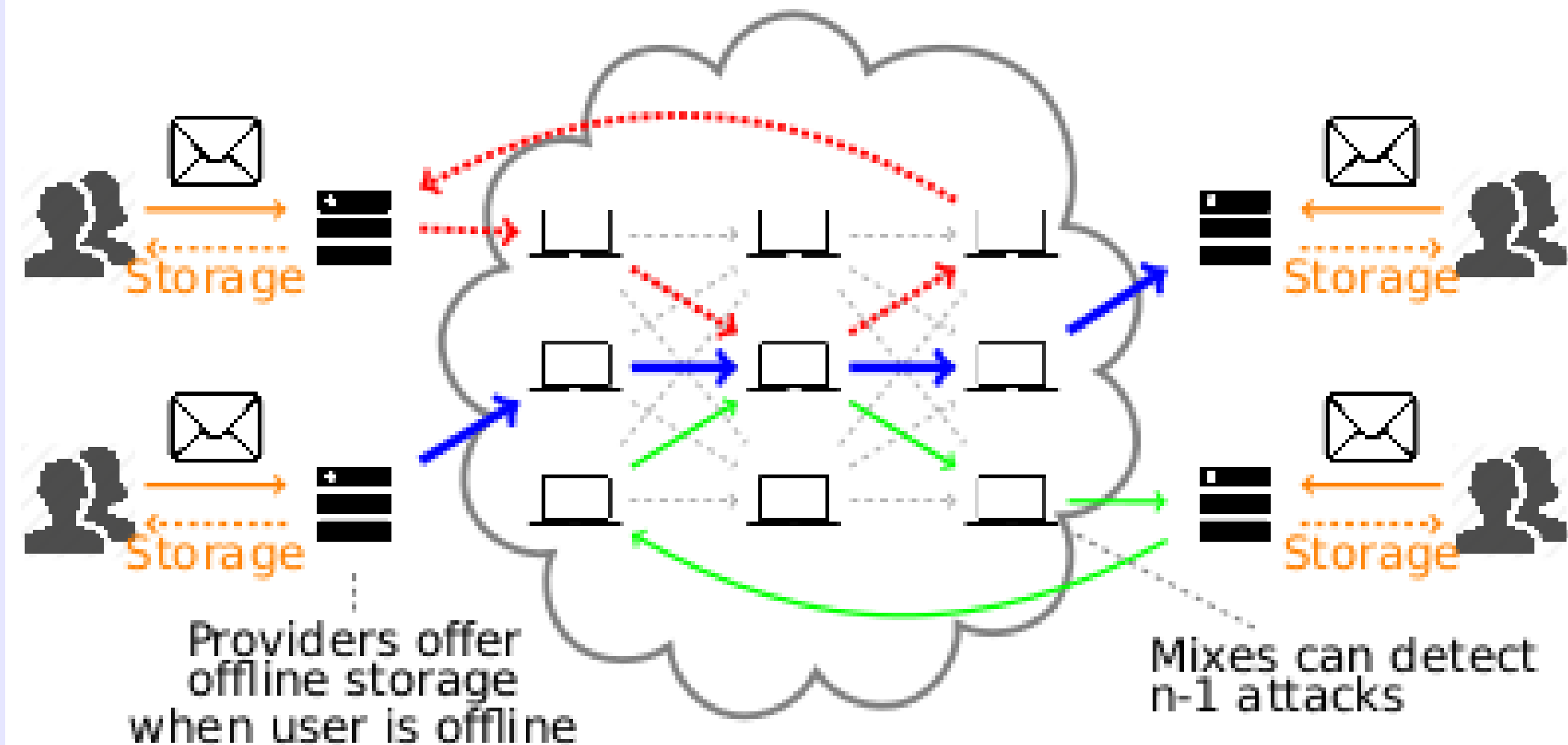
~~(1,Hi Larry,532105)~~
(1,Hi Bob,465231)
(2,Meet me at,782290)
~~(2,I'll call you at,793122)~~
~~(3,6PM,891231)~~
(3,7PM,344287)
~~(4,Yours-Susan,553419)~~
(4,Love-Alice,312265)



(1,Hi Larry,532105)
(1,Hi Bob,465231)
(2,Meet me at,782290)
(2,I'll call you at,793122)
(3,6PM,891231)
(3,7PM,344287)
(4,Yours-Susan,553419)
(4,Love-Alice,312265)

Obfuscation for unobservability: cover traffic in Loopix

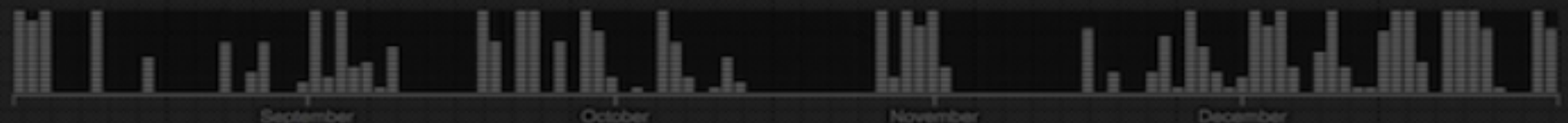
Users' loop cover traffic
generates traffic
in two directions



Obfuscation as adversarial response: Ad Nauseum



SINCE MONDAY AUGUST 4 10:22PM 2307 ADS CLICKED, OUT OF THE 2307 DETECTED.



promoted

age)
ceSwap /r/ThriftStoreHauls /r/doener 36 comments

n by Improved Contraceptive Use (H

a professional dog photographer. (Im

ssociated with your parents political

ur.com)

ame! (i.imgur.com)



CLICKED 5 / 6 ADS DETECTED = \$7.90²

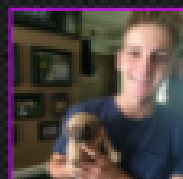
VIEW AD VAULT

11



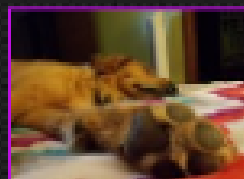
Welcome to WholesomeTube! - BREAKING THE GUIDELINES! - YouTube

www.youtube.com



i.redd.it/uploads.com

i.redd.it/uploads.com



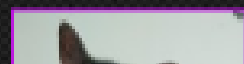
Sleepy high five - Album on Imgur

imgur.com



Imgur

i.imgur.com

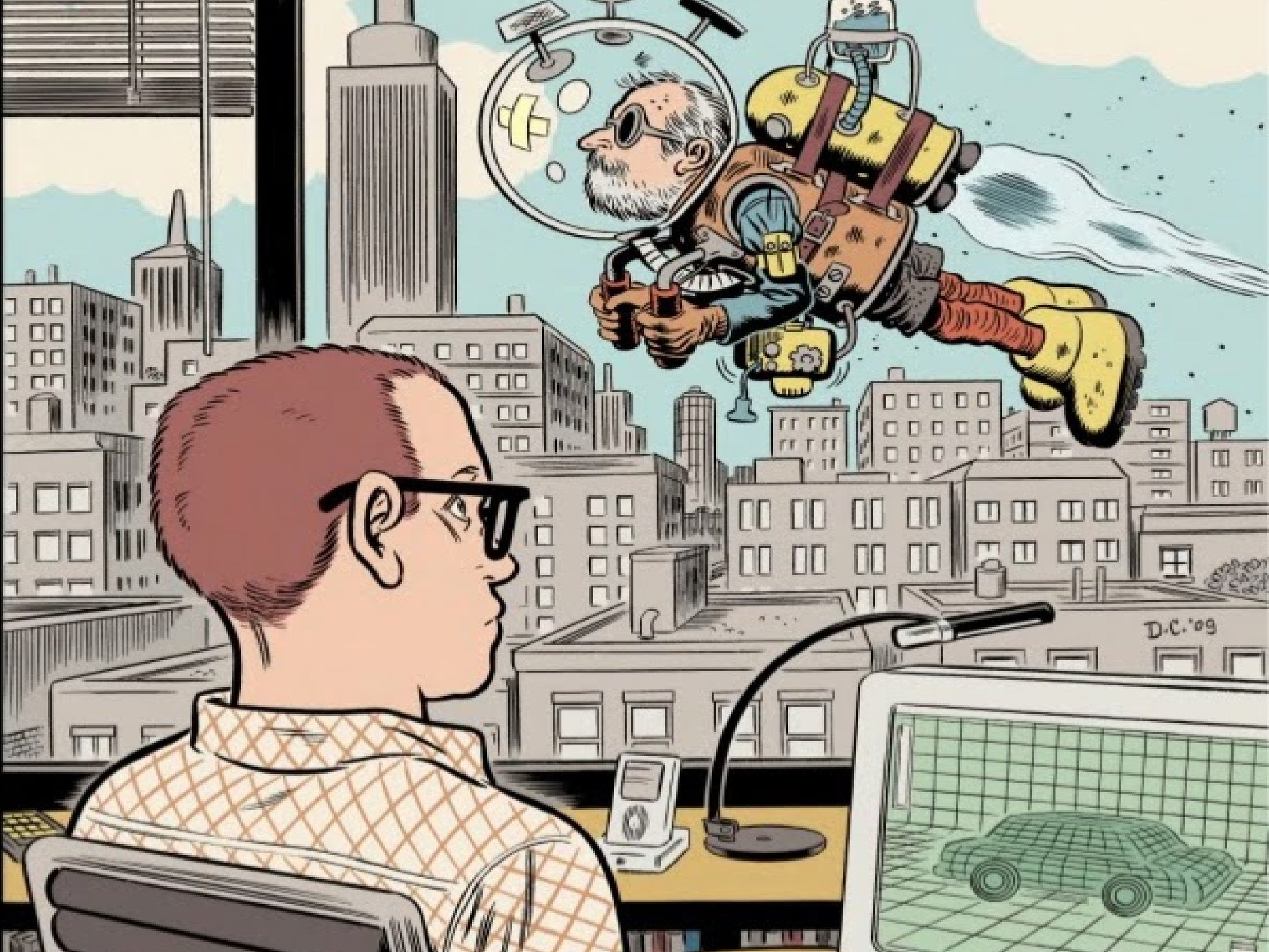


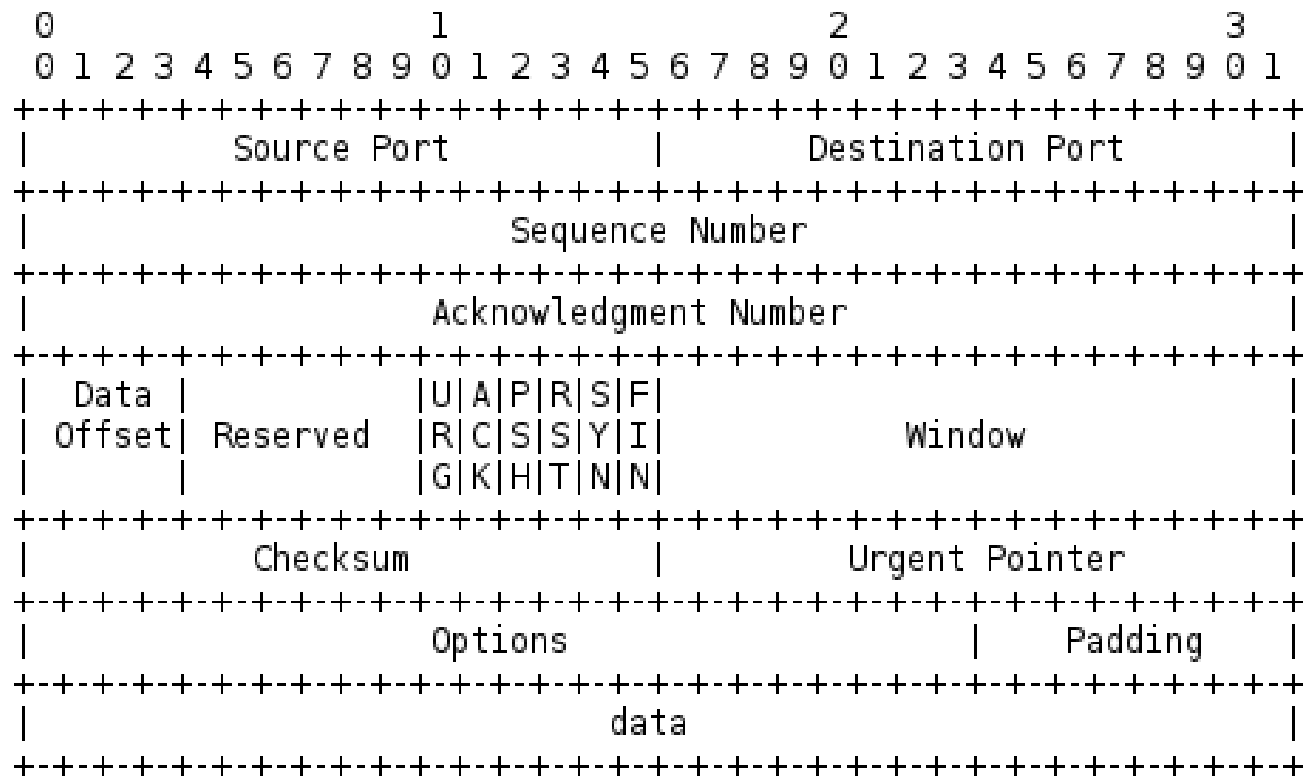
Imgur: The most awesome images on the

PAUSE ADNAUSEAM

SETTINGS







TCP Header Format