



Welcome to

# Digitalt selvforsvar og Masseeovervågnings-paranoia! feat. Peter Kofod

Henrik Lund Kramshøj [hlk@zecurity.dk](mailto:hlk@zecurity.dk)

Slides are available as PDF, [kramshoej@Github](mailto:kramshoej@Github)

# Planen idag



FreeFoto.com

KI 14-17 m pause

Mindre foredrag mere snak

Mindre enetale, mere foredrag 2.0 med socialt medie, informationsdeling og interaktion

Iaften Cryptoparty feat. Henrik Kramshøj, Peter Kofod m.fl.

# Formålet i dag



Don't Panic!

Introducere eksempler på trusler

Demonstrere hvordan overvågning i praksis kan lade sig gøre med det trådløse netværk som eksempel

Vi kommer til at sniffe på netværket

Sluk din telefon og laptops trådløse kort hvis du er paranoid ☺

# Joanna Rutkowska has a new iPhone



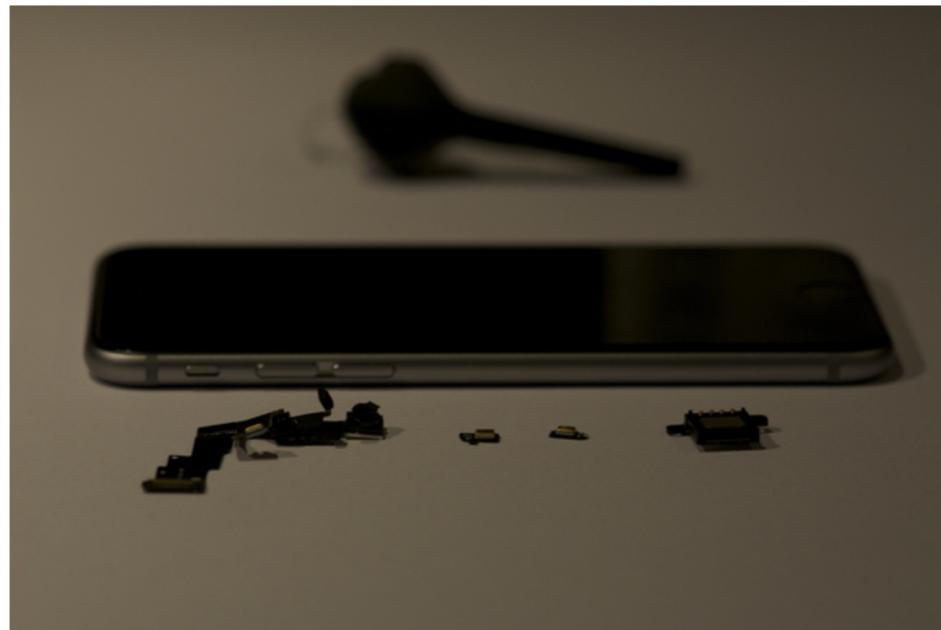
Joanna Rutkowska

@rootkovska



Following

My new iPhone. And all of its microphones.  
And the front camera ;)



This is what people do with their new phones now

# Jake Appelbaum Motorola Moto E



The Motorola Moto E (model: XT1021 and related devices) is an affordable modern Android cellphone. It may be purchased in cash at your local MediaMarkt for around 100 Euros. It is easy to modify for your everyday surveillance detection, counter-surveillance and anti-surveillance needs.

## Images of hardware before and after modification

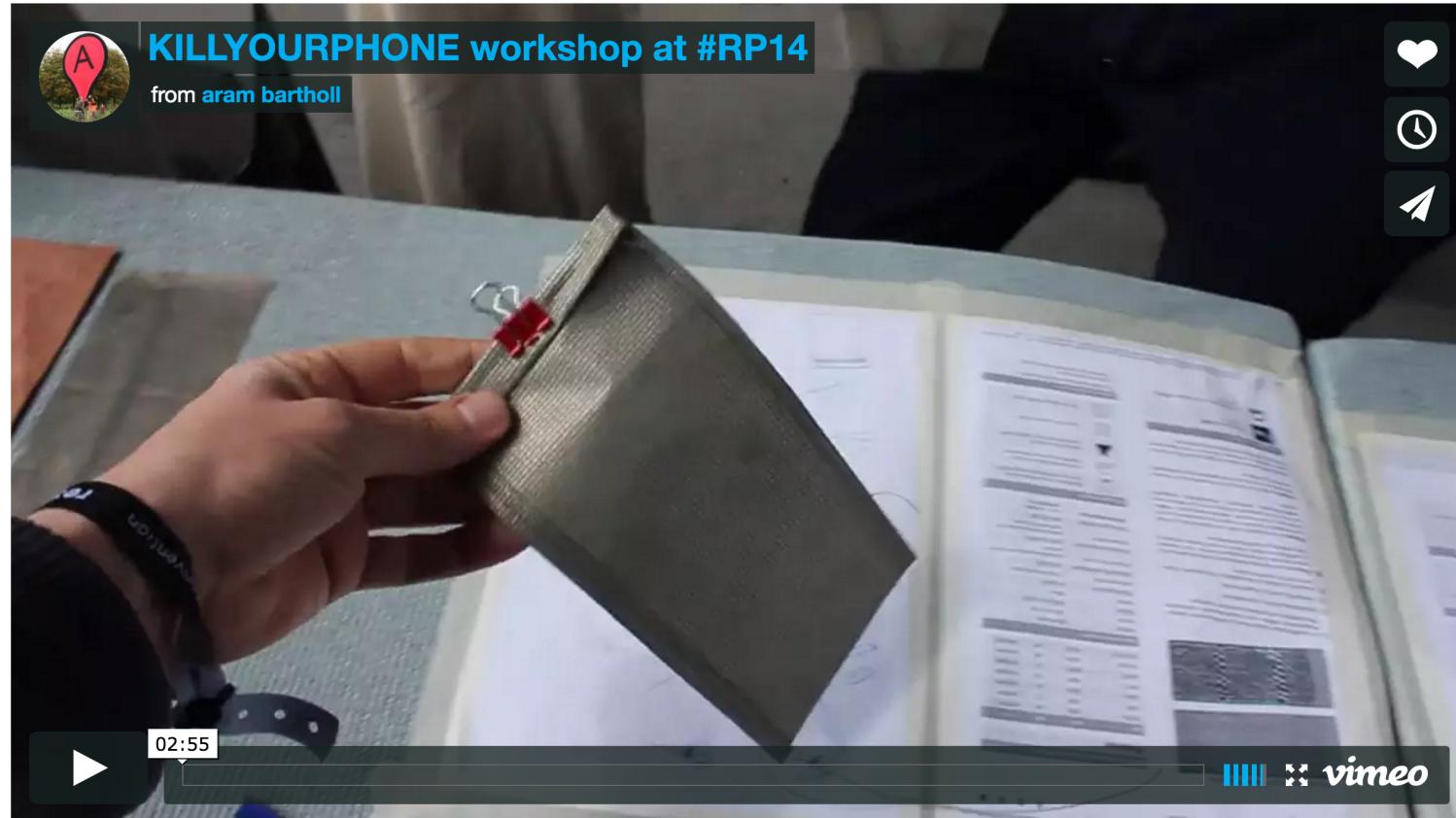


[https://people.torproject.org/~ioerror/skunkworks/moto\\_e/](https://people.torproject.org/~ioerror/skunkworks/moto_e/)

# Killyourphone: stop signalerne når vi fester



KILLYOURPHONE at [re:publica](#) conference Berlin, May 2014



<http://killyourphone.com/>

# Opfordring: Køb dine egne gadgets!



Hvis du køber dine egne enheder bestemmer du:

Modellen, fabrikat, features

Indstillerne: sikkerhedsindstillerne, fuld disk kryptering

Hvilke cloudservices du vil bruge

Hvilken backup service, hvor og hvordan

Bemærk mange dimser styrer vi ikke 100% - iPhone eksempelvis

Der er eksempler på at arbejdspladsen kan kræve du åbner en firma-laptop, for politiet

# Gode råd til jer



Brug teknologien

Lær teknologien at kende - læs manualen!

Tænk på følsomheden af data I gemmer og overfører

- Slå ting fra som I ikke bruger
- Slå bluetooth fra når I ikke bruger den
- Opdater softwaren på enheden
- Slå kryptering til hvor I kan: IMAPS, POP3S, HTTPS og over bluetooth
- Brug låsekode fremfor tastaturlås uden kode på mobiltelefonen
- Stol ikke for meget på fingertryksaflæsere

Gælder alle enheder og steder I gemmer data

# Hacking er magi



Hacking ligner indimellem magi

# Hacking er ikke magi



Hacking kræver blot lidt ninja-træning



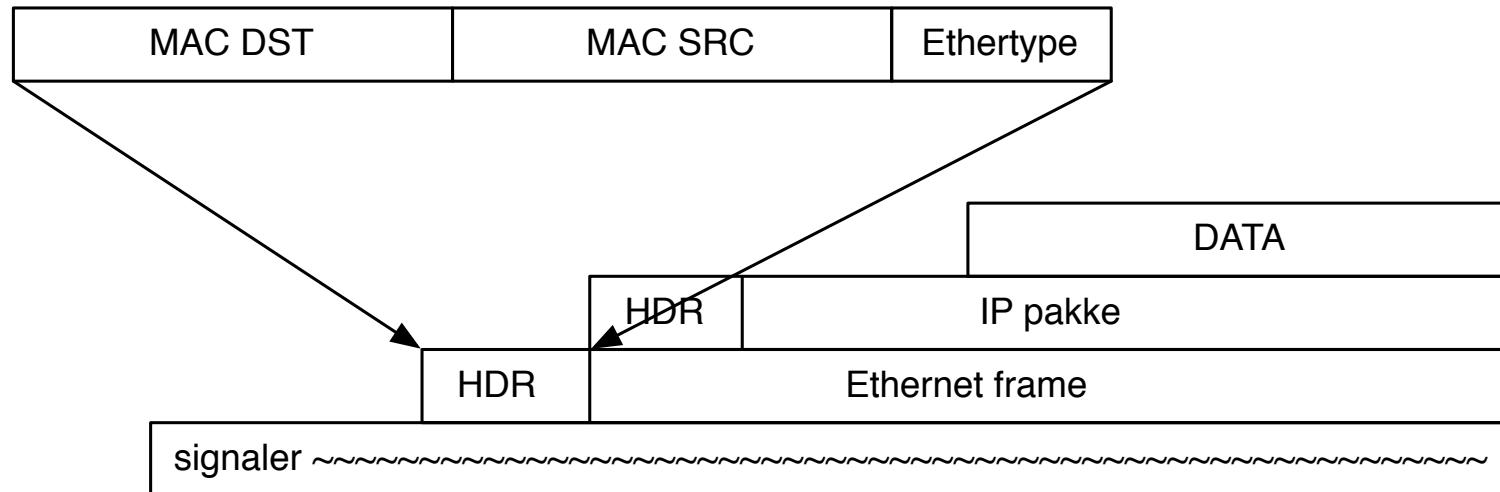
## Movie:Kryptonite lock - old

The image shows a YouTube video player interface. At the top left is the YouTube logo. The main frame displays a video thumbnail of a man with glasses and a white t-shirt, working on a bicycle lock. Below the video frame is a control bar with a play button, volume icon, and a progress bar indicating the video is at 1:57 of 2:28. Below the control bar is a title card with the text "How To Unlock a Kryptonite Lock With a Bic Pen".

Just search for: kryptonite lock bic pen

<https://www.youtube.com/watch?v=LahDQ2ZQ3e0>

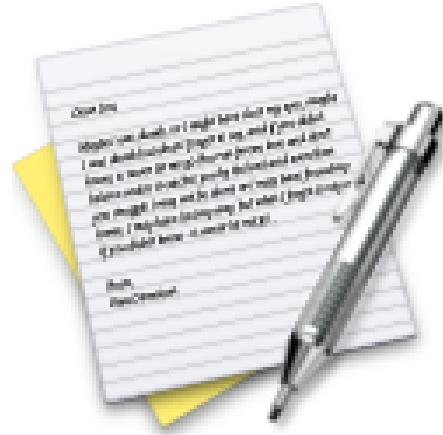
# Hacking eksempel - det er ikke magi



Mange af vores protokoller er åbne og usikre

Mange af vores programmer, apps og websites er usikre

# Øvelse: Snif på netværket



Jeg bruger Kali Linux til at lytte på det trådløse netværk

Vi starter med at se

- Hvor mange og hvilke systemer, fabrikat
- Hvad sker der på netværket, broadcast traffik
- passiv vs aktiv informationsindsamling
- Nmap scans og webservere
- og hvad der lige dukker op ☺



# Opsummering og client side anbefalinger

## Drive-by download

From Wikipedia, the free encyclopedia

**Drive-by download** means three things, each concerning the unintended download of computer software from the Internet:

1. Downloads which a person authorized but without understanding the consequences (e.g. downloads which install an unknown or counterfeit executable program, ActiveX component, or Java applet). This is usually caused by poor security design[clarification needed]. The user should not be frequently asked to accept security-critical decisions, often with very limited knowledge and within limited time.
2. Any download that happens without a person's knowledge.
3. Download of spyware, a computer virus or any kind of malware that happens without a person's knowledge.

Kan vi undvære Java, Flash og PDF?

SKAL din laptop hedde dit navn på netværket?

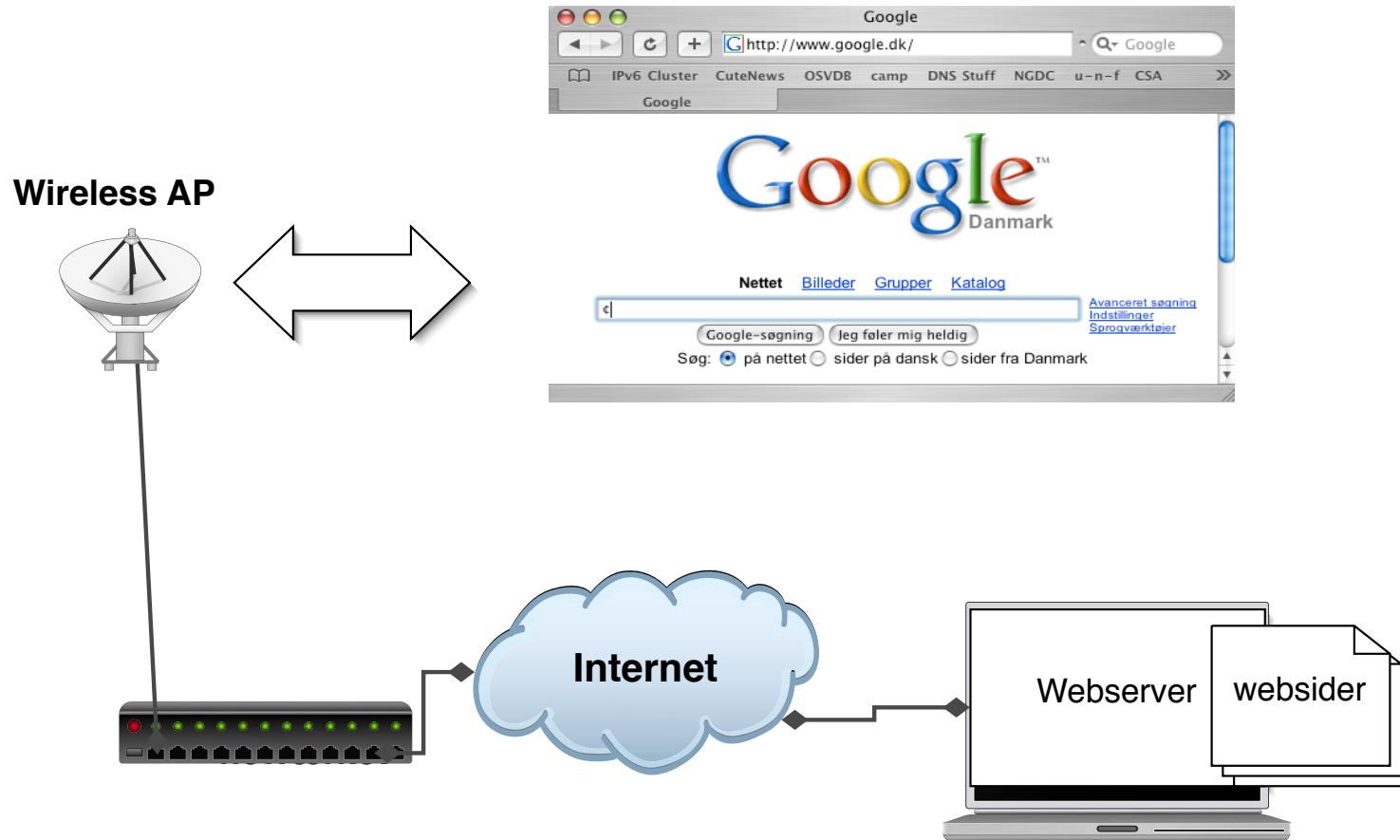
- Gå alle dine indstillinger igennem, tag dem med i aften, hjælp hinanden

Kilde: [https://en.wikipedia.org/wiki/Drive-by\\_download](https://en.wikipedia.org/wiki/Drive-by_download)

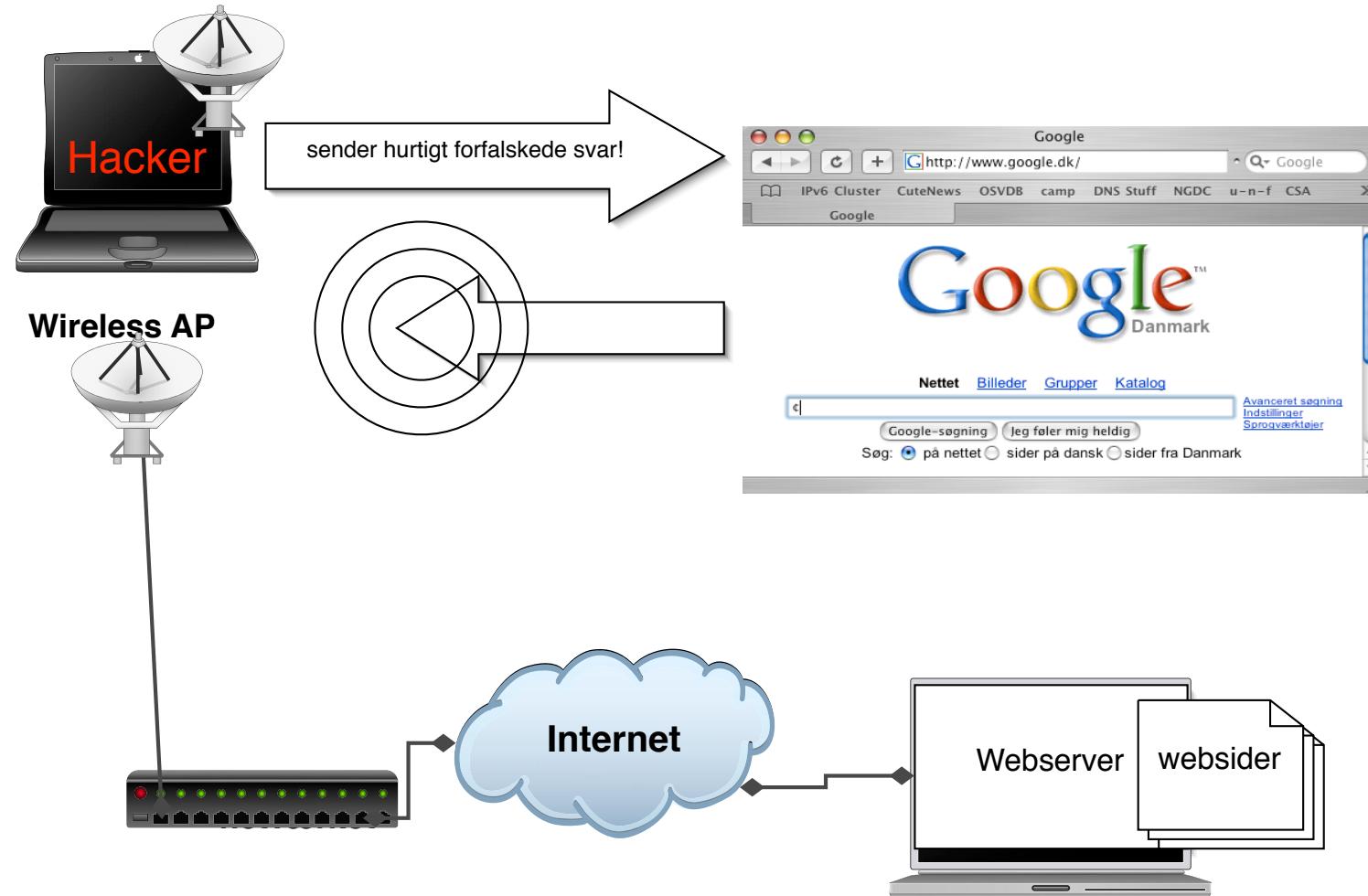
# HLK del 2. mere teknik



# Normal WLAN brug



# Packet injection - airpwn



# Hackerværktøjer



Vi kommer til at bruge hackerværktøjer

*Improving the Security of Your Site by Breaking Into it* af Dan Farmer og Wietse Venema i 1993

De udgav i 1995 så en softwarepakke med navnet SATAN *Security Administrator Tool for Analyzing Networks*

De forårsagede en del panik og furore, alle kan hacke, verden bryder sammen

We realize that SATAN is a two-edged sword – like many tools, it can be used for good and for evil purposes. We also realize that intruders (including wannabees) have much more capable (read intrusive) tools than offered with SATAN.

Kilde: <http://www.fish2.com/security/admin-guide-to-cracking.html>

# Brug hackerværktøjer!



Hackerværktøjer – bruger I dem? – efter dette kursus gør I

Portscannere kan afsløre huller i forsvaret

Webtestværktøjer som crawler igennem et website og finder alle forms kan hjælpe

I vil kunne finde mange potentielle problemer proaktivt ved regelmæssig brug af disse værktøjer – også potentielle driftsproblemer

Husk dog penetrationstest er ikke en sølvkugle

Honeypots kan måske være med til at afsløre angreb og kompromitterede systemer hurtigere

# Aftale om test af netværk

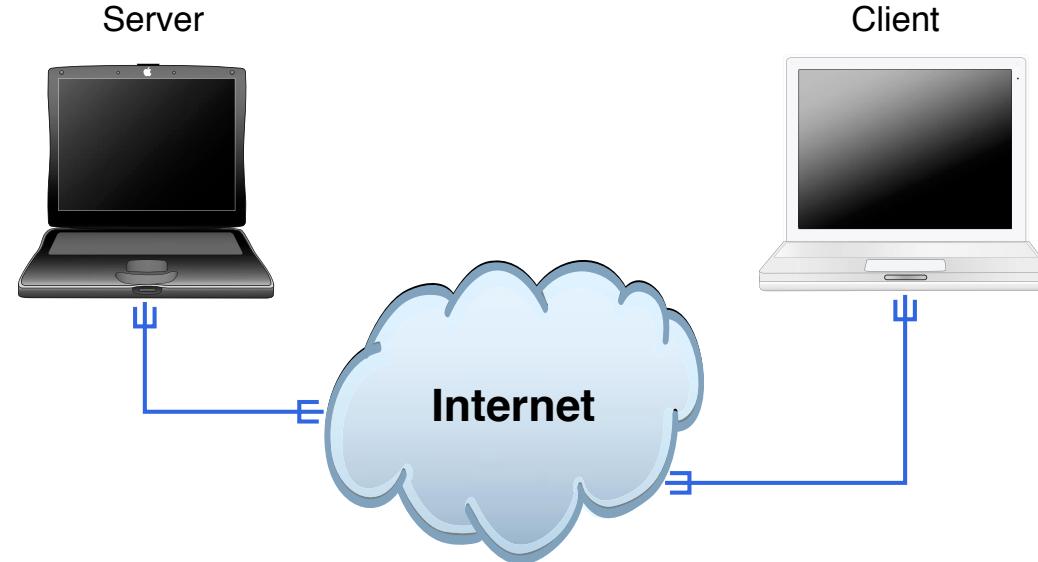


**Straffelovens paragraf 263 Stk. 2. Med bøde eller fængsel indtil 1 år og 6 måneder straffes den, der uberettiget skaffer sig adgang til en andens oplysninger eller programmer, der er bestemt til at bruges i et informationssystem.**

Hacking kan betyde:

- At man skal betale erstatning til personer eller virksomheder
- At man får konfiskeret sit udstyr af politiet
- At man, hvis man er over 15 år og bliver dømt for hacking, kan få en bøde – eller fængselsstraf i alvorlige tilfælde
- At man, hvis man er over 15 år og bliver dømt for hacking, får en plettet straffeattest. Det kan give problemer, hvis man skal finde et job eller hvis man skal rejse til visse lande, fx USA og Australien
- Frygten for terror har forstærket ovenstående – så lad være!

# Internet idag



Klienter og servere

Rødder i akademiske miljøer

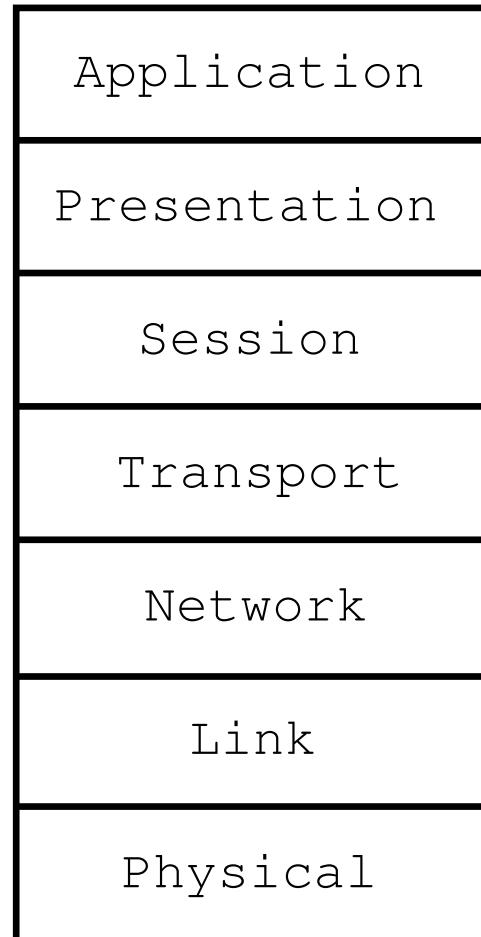
Protokoller der er op til 20 år gamle

Meget lidt kryptering, mest på http til brug ved e-handel

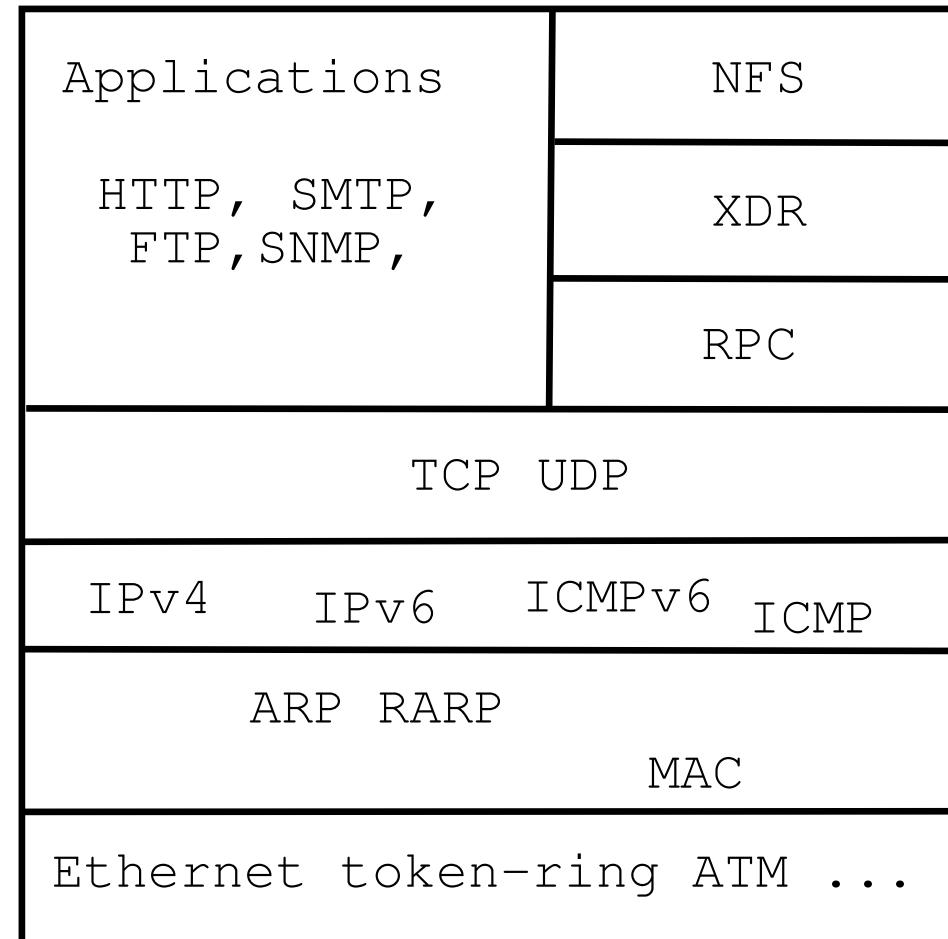
# OSI og Internet modellerne



OSI Reference Model



Internet protocol suite





# Most vulnerable operating systems in 2014

Operating system	# of vulnerabilities	# of HIGH vulnerabilities	# of MEDIUM vulnerabilities	# of LOW vulnerabilities
Apple Mac OS X	147	64	67	16
Apple iOS	127	32	72	23
Linux Kernel	119	24	74	21
Microsoft Windows Server 2008	38	26	12	0
Microsoft Windows 7	36	25	11	0
Microsoft Windows Server 2012	38	24	14	0
Microsoft Windows 8	36	24	12	0
Microsoft Windows 8.1	36	24	12	0
Microsoft Windows Vista	34	23	11	0
Microsoft Windows RT	30	22	8	0

An average of 19 vulnerabilities per day were reported in 2014, according to the data from the National Vulnerability Database (NVD).

Source:

<http://www.gfi.com/blog/most-vulnerable-operating-systems-and-applications-in-2014/>



# Most vulnerable applications in 2014

Application	# of vulnerabilities	# of HIGH vulnerabilities	# of MEDIUM vulnerabilities	# of LOW vulnerabilities
Microsoft Internet Explorer	242	220	22	0
Google Chrome	124	86	38	0
Mozilla Firefox	117	57	57	3
Adobe Flash Player	76	65	11	0
Oracle Java	104	50	46	8
Mozilla Thunderbird	66	36	29	1
Mozilla Firefox ESR	61	35	25	1
Adobe Air	45	38	7	0
Apple TV	86	29	49	8
Adobe Reader	44	37	7	0
Adobe Acrobat	43	35	8	0
Mozilla SeaMonkey	63	28	34	1

Not surprisingly at all, web browsers continue to have the most security vulnerabilities because they are a popular gateway to access a server and to spread malware on the clients.

## Source:

<http://www.gfi.com/blog/most-vulnerable-operating-systems-and-applications-in-2014/>

# April 2014: Heartbleed hacking



```
06b0: 2D 63 61 63 68 65 0D 0A 43 61 63 68 65 2D 43 6F -cache..Cache-Co
06c0: 6E 74 72 6F 6C 3A 20 6E 6F 2D 63 61 63 68 65 0D ntrol: no-cache.
06d0: 0A 0D 0A 61 63 74 69 6F 6E 3D 67 63 5F 69 6E 73 ...action=gc_in
06e0: 65 72 74 5F 6F 72 64 65 72 26 62 69 6C 6C 6E 6F ert_order&billno
06f0: 3D 50 5A 4B 31 31 30 31 26 70 61 79 6D 65 6E 74 =PZK1101&payment
0700: 5F 69 64 3D 31 26 63 61 72 64 5F 6E 75 6D 62 65 _id=1& card'numbe
0710: XX r=4060xxxx413xxx
0720: 39 36 26 63 61 72 64 5F 65 78 70 5F 6D 6F 6E 74 96&card'exp'mont
0730: 68 3D 30 32 26 63 61 72 64 5F 65 78 70 5F 79 65 h=02&card'exp'ye
0740: 61 72 3D 31 37 26 63 61 72 64 5F 63 76 6E 3D 31 ar=17&card'cvn=1
0750: 30 39 F8 6C 1B E5 72 CA 61 4D 06 4E B3 54 BC DA 09.l...r.aM.N.T..
```

- Obtained using Heartbleed proof of concepts - Gave full credit card details
- "can XXX be exploited- yes, clearly! PoCs ARE needed without PoCs even Akamai wouldn't have repaired completely!"
- The internet was ALMOST fooled into thinking getting private keys from Heartbleed was not possible - scary indeed.

# September 2015: Heartbleed vulnerable servers



**John Matherly**  
@achillean

[Follow](#)

FYI: there are still more than 200,000 devices  
on the Internet vulnerable to Heartbleed

#### TOP COUNTRIES



United States	57,272
Germany	21,660
China	11,300
France	10,094
United Kingdom	9,125

#### TOP SERVICES

HTTPS	174,020
HTTPS (8443)	23,621
Webmin	8,148
8081	1,981
Symantec Data Center Security	1,307

Source: Data from Shodan and Shodan Founder John Matherly

# Getting to your data: Google for it



Google Search: filetype:dat "password.dat"  
http://www.google.com/search?hl=en&lr=&ie=UTF8

IPv6 Cluster CuteNews OSVDB camp DNS Stuff NGDC u-n-f CSA

Google Search: filetype:dat ...

Web Images Groups News Froogle more »  
filetype:dat "password.dat" Search Advanced Se Preferences

**Web** Results 1 - 10 of about 22 for filetype:dat "password.dat". (0.28 seconds)

#User and passwords #Mon Oct 29 11:39:19 EST 2001 guest4=guest4 ...  
#User and passwords #Mon Oct 29 11:39:19 EST 2001 guest4=guest4 guest1=guest1  
guest3=guest3 guest2=guest2 guest5=guest5 guest6=guest6 guest7=guest7 guest8 ...  
[www.ils.unc.edu/isee/demo/config/password.dat](http://www.ils.unc.edu/isee/demo/config/password.dat) - 1k - [Cached](#) - [Similar pages](#)

**CVS log for mrdatae/Attic/password.dat**  
CVS log for mrdatae/Attic/**password.dat**. Help. (back) Up to [d0cvs] / mrdatae Request  
diff between arbitrary revisions / Display revisions graphically ...  
[www-d0.fnal.gov/cgi-bin/cvsweb.cgi/mrdatae/Attic/password.dat](http://www-d0.fnal.gov/cgi-bin/cvsweb.cgi/mrdatae/Attic/password.dat) - 12k - [Cached](#) - [Similar pages](#)

Google as a hacker tool? oprindeligt beskrevet af Johnny Long

Concept named **googledorks** when google indexes information not supposed to be public <http://www.exploit-db.com/google-dorks/>

# Kali Linux the new backtrack



The most advanced penetration testing distribution, ever.

From the creators of BackTrack comes Kali Linux, the most advanced and versatile penetration testing distribution ever created. BackTrack has grown far beyond its humble roots as a live CD and has now become a full-fledged operating system. With all this buzz, you might be asking yourself: - [What's new ?](#)

Kali – <https://www.kali.org/> version 2.0 netop udkommet!

Wireshark – <https://www.wireshark.org> avanceret netværkssniffer

# Wireshark – grafisk pakkesniffer



We're having a conference! You're invited!

**WIRESHARK**

Get Acquainted ▾ Get Help ▾ Develop ▾

Sharkfest '15 Our Sponsor WinPcap

**Download**  
Get Started Now

**Learn**  
Knowledge is Power

**Enhance**  
With Riverbed Technology

**News And Events**

**Join us at SHARKFEST '15!**  
SHARKFEST '15 will be held from June 22 – 25 at the Computer History Museum in Mountain View, CA.  
[Learn More ▶](#)

**Troubleshooting with Wireshark**  
By Laura Chappell  
Foreword by Gerald Combs  
Edited by Jim Aragon  
This book focuses on the tips and techniques used to identify

**Wireshark Blog**

**Cool New Stuff**  
Dec 17 | By Evan Huus

**Wireshark 1.12 Officially Released!**  
Jul 31 | By Evan Huus

**To Infinity and Beyond! Capturing Forever with Tshark**  
Jul 8 | By Evan Huus

[More Blog Entries ▶](#)

**Enhance Wireshark**

Riverbed is Wireshark's primary sponsor and provides our funding. [They also make great products.](#)

**802.11 Packet Capture**

- WLAN packet capture and transmission
- Full 802.11 a/b/g/n support
- View management, control and data frames
- Multi-channel aggregation (with multiple adapters)

[Learn More ▶](#)

[Buy Now ▶](#)

<https://www.wireshark.org>  
Både til Windows og Unix



# Brug af Wireshark

http-example.cap

Apply a display filter ... <%>

No.	Time	Source	Destination	Protocol	Info
1	0.000000	172.24.65.102	91.102.91.18	TCP	58816 - http [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=16 TStamp=745562412 TSectr=0 SACK_PERM...
2	0.000170	172.24.65.102	91.102.91.18	TCP	58817 - http [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=16 TStamp=745562412 TSectr=0 SACK_PERM...
3	0.127053	91.102.91.18	172.24.65.102	TCP	http - 58816 [SYN, ACK] Seq=1 Ack=1 Win=16384 Len=0 MSS=1460 SACK_PERM=1 WS=8 TStamp=18552...
4	0.127167	91.102.91.18	172.24.65.102	TCP	http - 58817 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0 MSS=1460 SACK_PERM=1 WS=8 TStamp=25124...
5	0.127181	172.24.65.102	91.102.91.18	TCP	58816 - http [ACK] Seq=1 Ack=1 Win=131760 Len=0 TStamp=745562538 TSectr=1855239975
6	0.127226	172.24.65.102	91.102.91.18	TCP	58817 - http [ACK] Seq=1 Ack=1 Win=131760 Len=0 TStamp=745562538 TSectr=2512433851
7	0.127363	172.24.65.102	91.102.91.18	HTTP	GET / HTTP/1.1
8	0.141320	91.102.91.18	172.24.65.102	HTTP	HTTP/1.1 304 Not Modified
9	0.141421	172.24.65.102	91.102.91.18	TCP	58816 - http [ACK] Seq=503 Ack=190 Win=131568 Len=0 TStamp=745562551 TSectr=1855239975

▶ Frame 7: 568 bytes on wire (4544 bits), 568 bytes captured (4544 bits)  
▶ Ethernet II, Src: Apple\_6c:87:5e (7c:d1:c3:6c:87:5e), Dst: Cisco\_32:09:30 (44:2b:03:32:09:30)  
▶ Internet Protocol Version 4, Src: 172.24.65.102 (172.24.65.102), Dst: 91.102.91.18 (91.102.91.18)  
▶ Transmission Control Protocol, Src Port: 58816 (58816), Dst Port: http (80), Seq: 1, Ack: 1, Len: 502

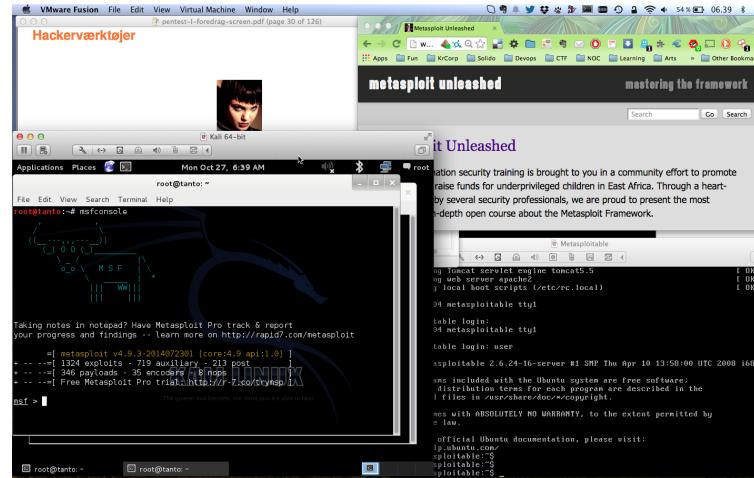
▼ Hypertext Transfer Protocol  
  ▶ GET / HTTP/1.1\r\n    Host: 91.102.91.18\r\n    Connection: keep-alive\r\n    Cache-Control: max-age=0\r\n    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,\*/\*;q=0.8\r\n    User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_9\_2) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.146 Safari/537.36\r\n    Accept-Encoding: gzip,deflate,sdch\r\n    Accept-Language: en-US,en;q=0.8,cs;q=0.6,da;q=0.4\r\n    If-None-Match: "7053a63e31516a5bb27a295edb31d07524a6e0a3"\r\n    If-Modified-Since: Tue, 17 Nov 2009 11:22:22 GMT\r\n\r\n    [Full request URI: http://91.102.91.18/]  
    [HTTP request 1/1]  
    [Response in frame: 8]

0000 44 2b 03 32 09 30 7c d1 c3 6c 87 5e 08 00 45 00 D+.2.0|Äl.^..E.  
0010 02 2a 9e d7 40 00 40 06 f5 ff ac 18 41 66 5b 66 .\*.x@.ö~.At[f  
0020 5b 12 e5 c0 00 50 08 ea 0e c7 03 14 0c 19 80 18 [,.å,P.é.ç.....  
0030 20 2b 0f c0 00 00 01 01 08 0a 2c 70 61 aa 6e 94 +.À....,pañ.  
0040 b7 27 47 45 54 20 2f 20 48 54 54 58 2f 31 2e 31 .'GET / HTTP/1.1  
0050 0d 0a 48 6f 73 74 3a 20 39 31 2e 31 30 32 2e 39 ..Host: 91.102.9  
0060 31 2e 31 38 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e 1.18..Co nnection  
0070 3a 2b 6b 65 65 3d 30 0d 0a 41 63 63 65 70 74 3a 20 : keep-a live..Ca  
0080 63 68 65 2d 43 6f 6e 74 72 6f 6e 3a 20 6a 61 78 cheCont rol: max  
0090 2d 63 67 65 3d 30 0d 0a 41 63 63 65 70 74 3a 20 -age=0.. Accept:  
00a0 74 65 78 74 2f 68 74 6d 6c 2c 61 70 70 6c 69 63 text/htm l,appli  
00b0 61 74 69 6f 6e 2f 78 68 74 6d 6c 2b 78 6d 6c 2c ation/xh tml+xml,  
00c0 61 70 70 6c 69 63 61 74 69 6f 6e 2f 78 6d 6c 3b applicat ion/xml;

Packets: 9 · Displayed: 9 · Marked: 0 · Load time: 0:0:0 · Profile: Default

Læg mærke til filtermulighederne

# Hackerlab opsætning



- Hardware: en moderne laptop med CPU der kan bruge virtualisering  
Husk at slå virtualisering til i BIOS
- Software: dit favoritoperativsystem, Windows, Mac, Linux
- Virtualiseringssoftware: VMware, Virtual box, vælg selv
- Hackersoftware: Kali som Virtual Machine <https://www.kali.org/>
- Soft targets: Metasploitable, Windows 2000, Windows XP, ...



# Konsulentens udstyr wireless



Varenummer: 2225730

## TP-Link TL-WN722N

Hi-Speed USB - 802.11b, 802.11g, 802.11n

På lager, 1-2 dages levering  
( Billigste fragt: 0 kr. )  
[Ret land](#)

Køb

120,00 kr.

(96,00 kr.)

4 stk på lager i Århus  
0 stk på lager i Viborg  
0 stk på lager i København

Laptop or Netbook, I typically use USB wireless cards  
**NB: de indbyggede er ofte ringe - så check før køb ;-)**

Access Points - get a small selection for testing

Books:

- Kali Linux Wireless Penetration Testing: Beginner's Guide Beginner's Guide, Vivek Ramachandran, Cameron Buchanan, March 2015  
Also checkout his home page <http://www.vivekramachandran.com/>

# Kali Nethunter



- **802.11 Wireless Injection** and **AP mode** support with multiple supported USB wifi cards.
- Capable of running **USB HID Keyboard attacks**, much like the **Teensy** device is able to do.
- **Supports BadUSB MITM attacks**. Plug in your Nethunter to a victim PC, and have your traffic relayed through it.
- Contains a **full Kali Linux toolset**, with many tools available via a simple menu system.
- **USB Y-cable support** in the Nethunter kernel – use your OTG cable while still charging your Nexus device!
- **Software Defined Radio support**. Use **Kali Nethunter** with your HackRF to explore the wireless radio space.

Source: <https://www.kali.org/kali-linux-nethunter/>

# Kursusudbud, eksempelvis Kryptografi på Stanford



A promotional graphic for a Stanford University cryptography course on Coursera. The background is light grey. At the top left is the Stanford University logo. In the center is the word "Cryptography". To the right is a large image of a combination padlock. At the bottom left is a blue button with the text "Enroll / Login Now" and the subtext "Enroll in this online class for free with a Coursera account". At the top right is the text "Professor Dan Boneh" followed by "Computer Science Department Stanford University".

STANFORD  
UNIVERSITY

Cryptography

**Enroll / Login Now**  
Enroll in this online class for free with a Coursera account

Professor Dan Boneh  
Computer Science Department  
Stanford University

Åbent kursus på Stanford  
<http://crypto-class.org/>

# Questions?



Henrik Lund Kramshøj [hlk@zencurity.dk](mailto:hlk@zencurity.dk)

Need DDoS testing or pentest, ask me!

You are always welcome to send me questions later via email

Did you notice how a lot of the links in this presentation use HTTPS - encrypted