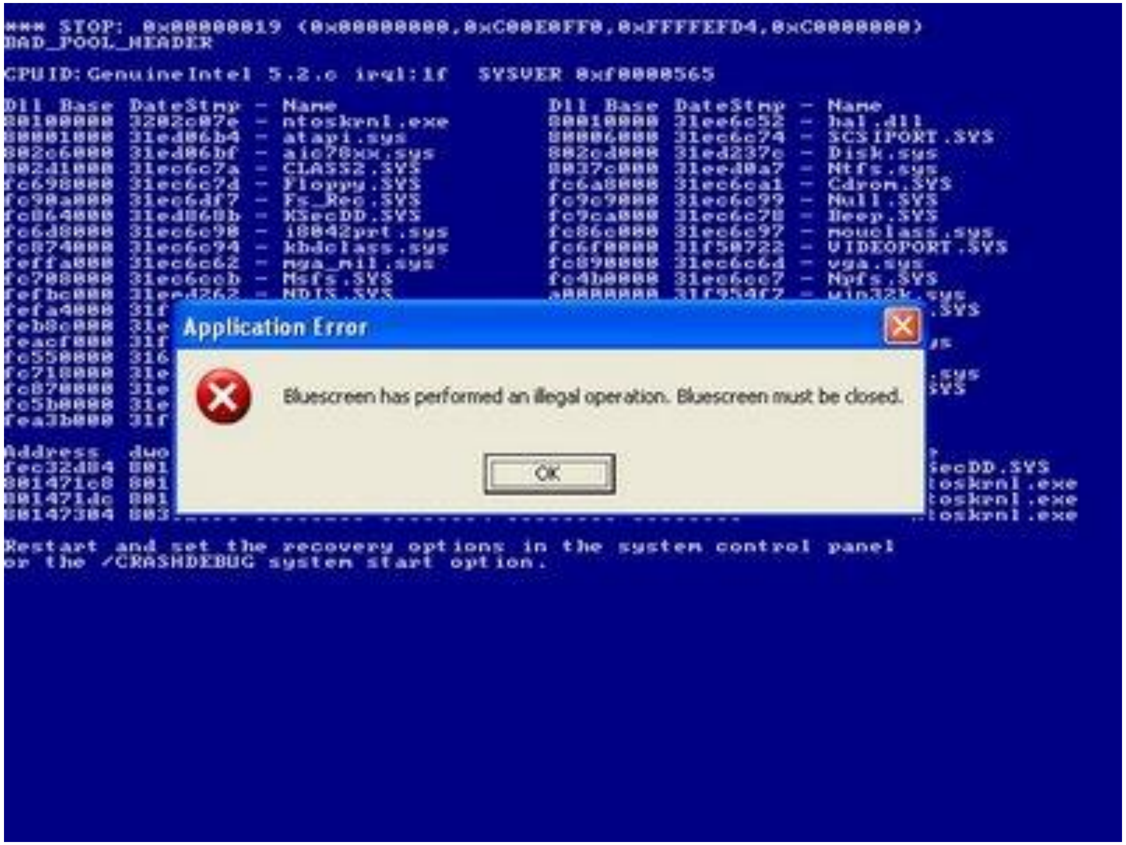
Mindset



```
*** STOP: 0x00000019 (0x00000000,0xC00E0FF0,0xFFFFEFD4,0xC0000000)
BAD_POOL_HEADER

CPUID:GenuineIntel 5.2.c irql:1f  SYSVER 0xf0000565

Dll Base DateStmp - Name                 Dll Base DateStmp - Name
80100000 3202c07e - ntoskrnl.exe         80010000 31ee6c52 - hal.dll
80001000 31ed06b4 - atapi.sys            80006000 31ec6c74 - SCSIPORT.SYS
802c6000 31ed06bf - aic78xx.sys          802cd000 31ed237c - Disk.sys
802d1000 31ec6c7a - CLASS2.SYS           8037c000 31eed0a7 - Ntfs.sys
fc698000 31ec6c7d - Floppy.SYS           fc6a8000 31ec6ca1 - Cdrom.SYS
fc90a000 31ec6df7 - Fs_Rec.SYS           fc9c9000 31ec6c99 - Null.SYS
fc864000 31ed868b - KSecDD.SYS           fc9ca000 31ec6c78 - Beep.SYS
fc6d8000 31ec6c90 - i8042prt.sys         fc86c000 31ec6c97 - mouclass.sys
fc874000 31ec6c94 - kbdclass.sys         fc6f0000 31f50722 - VIDEOPORT.SYS
feffa000 31ec6c62 - mga_mil.sys          fc890000 31ec6c6d - vga.sys
fc708000 31ec6ccb - Msfs.SYS             fc4b0000 31ec6cc7 - Npfs.SYS
fefbc000 31eed262 - NDIS.SYS             a0000000 31f954f7 - win32k.sys
fefa4000 31f                                                     .SYS
feb8c000 31e
feacf000 31f                                                     ys
fc550000 316
fc718000 31e                                                     .sys
fc870000 31e                                                     SYS
fc5b0000 31e
fea3b000 31f

Address  dwo                                                     ?
fec32d84 801                                                     SecDD.SYS
801471c8 801                                                     toskrnl.exe
801471dc 801                                                     toskrnl.exe
80147304 803                                                     toskrnl.exe

Restart and set the recovery options in the system control panel
or the /CRASHDEBUG system start option.
```

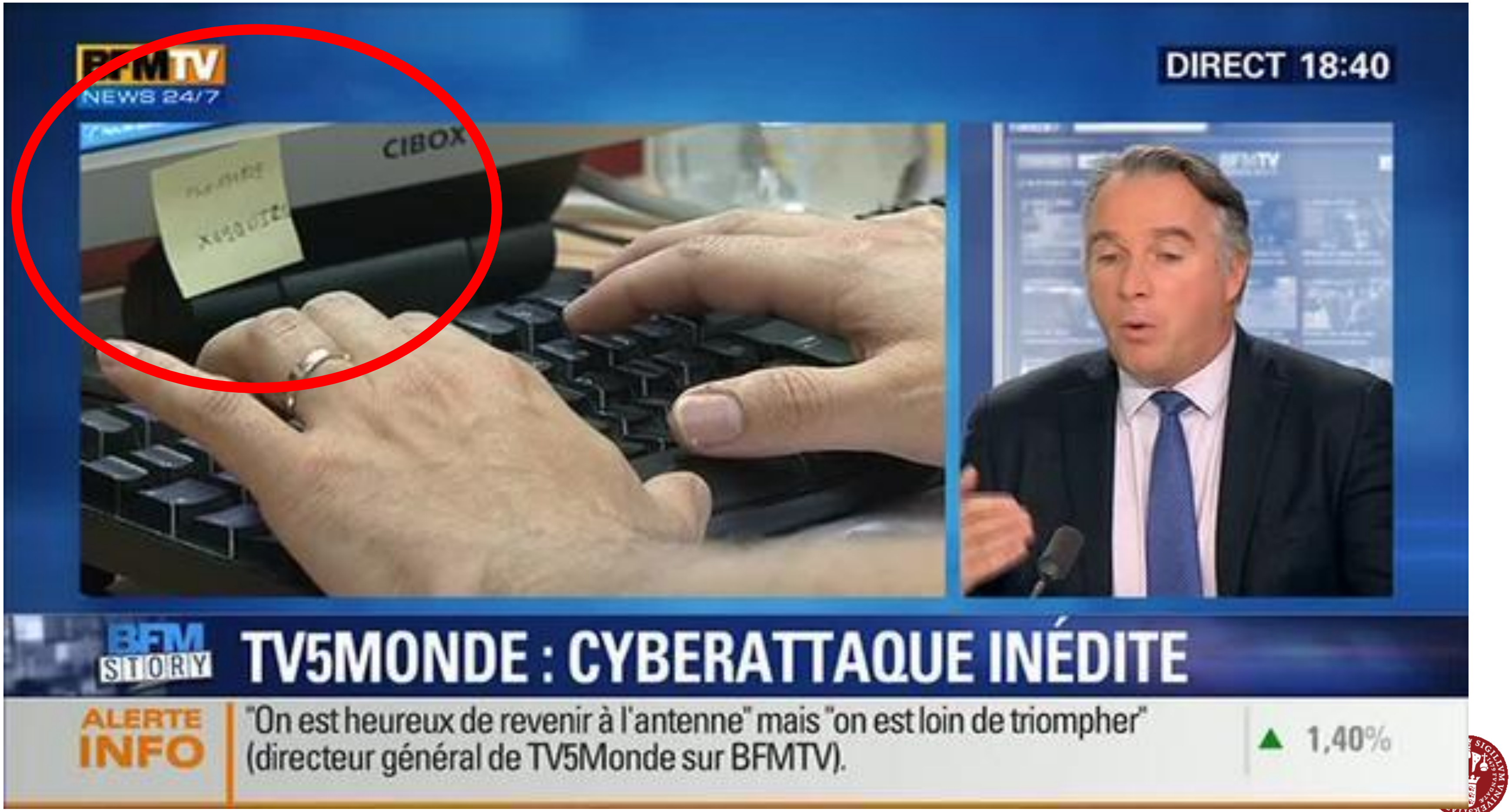
Bluescreen has performed an illegal operation. Bluescreen must be closed.

User

Administrator

IT Security

IT-security is fun (but not easy)

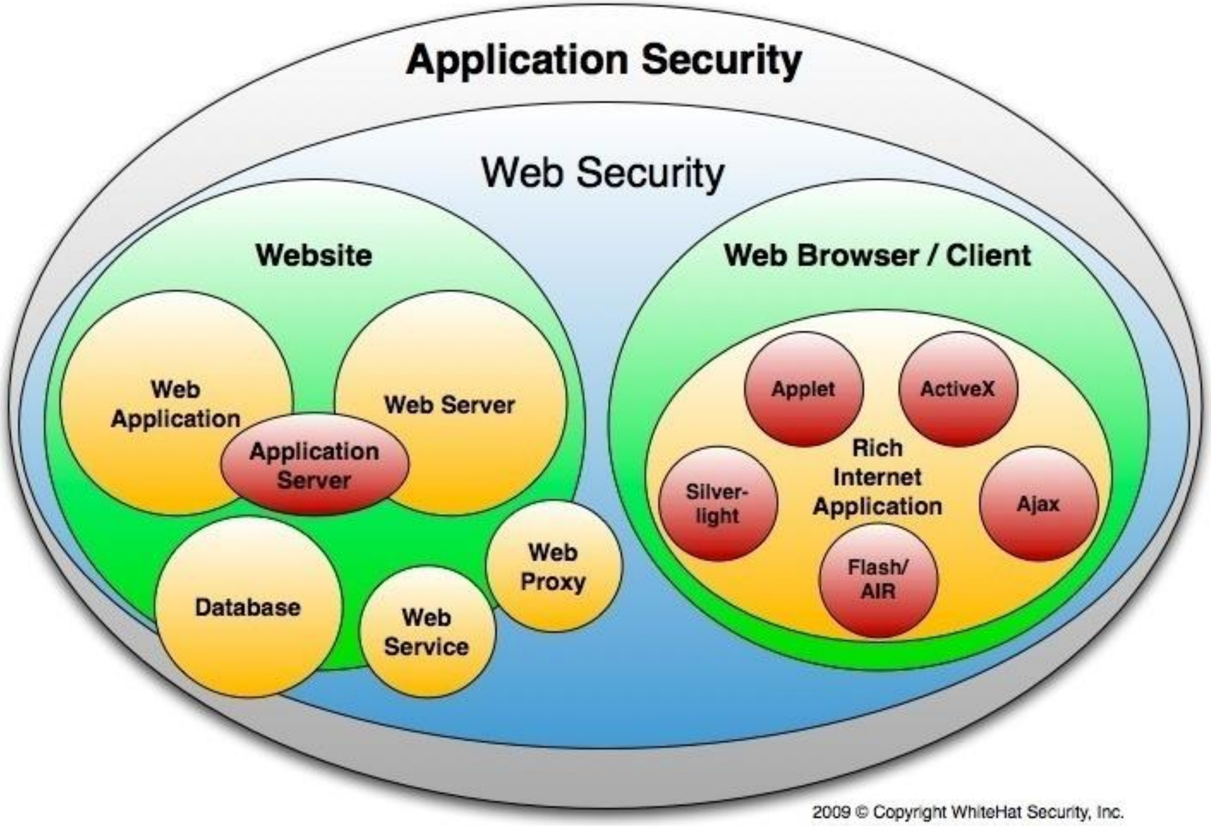


TV5MONDE : CYBERATTAQUE INÉDITE

"On est heureux de revenir à l'antenne" mais "on est loin de triompher" (directeur général de TV5Monde sur BFMTV).

IT Security is difficult

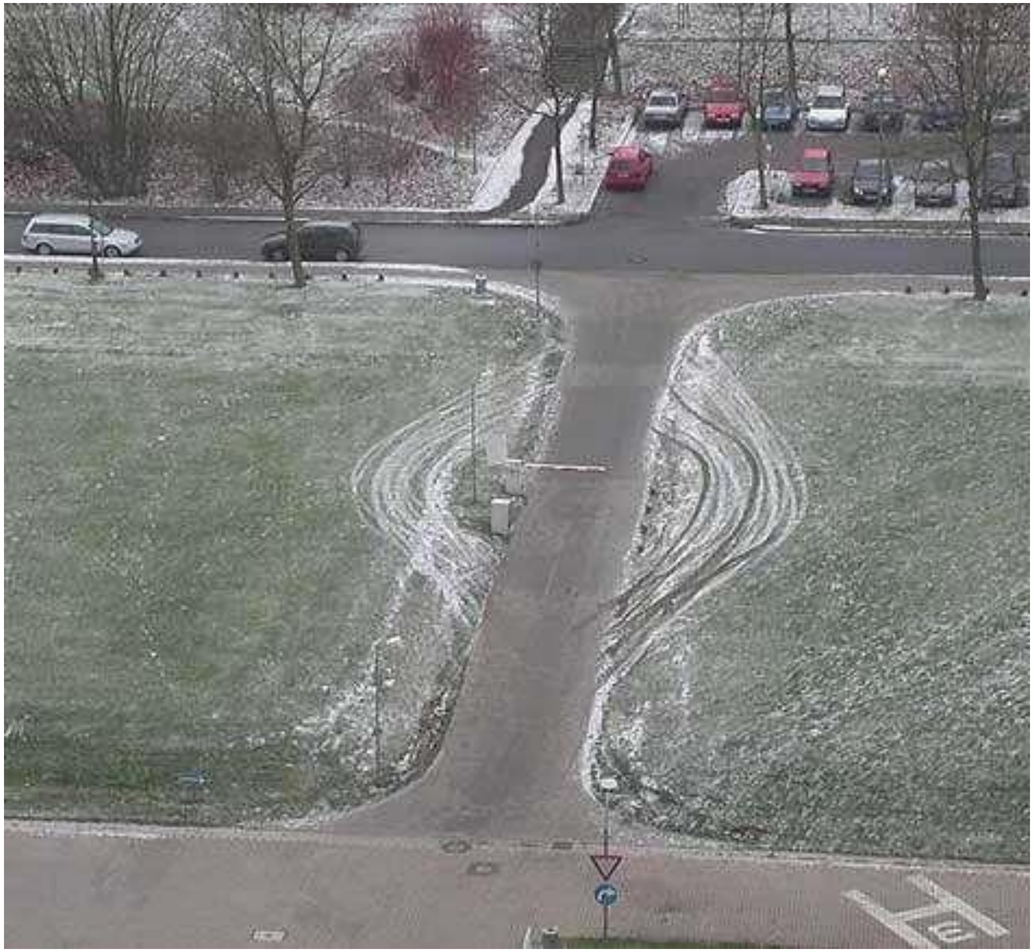
IT-security is complex



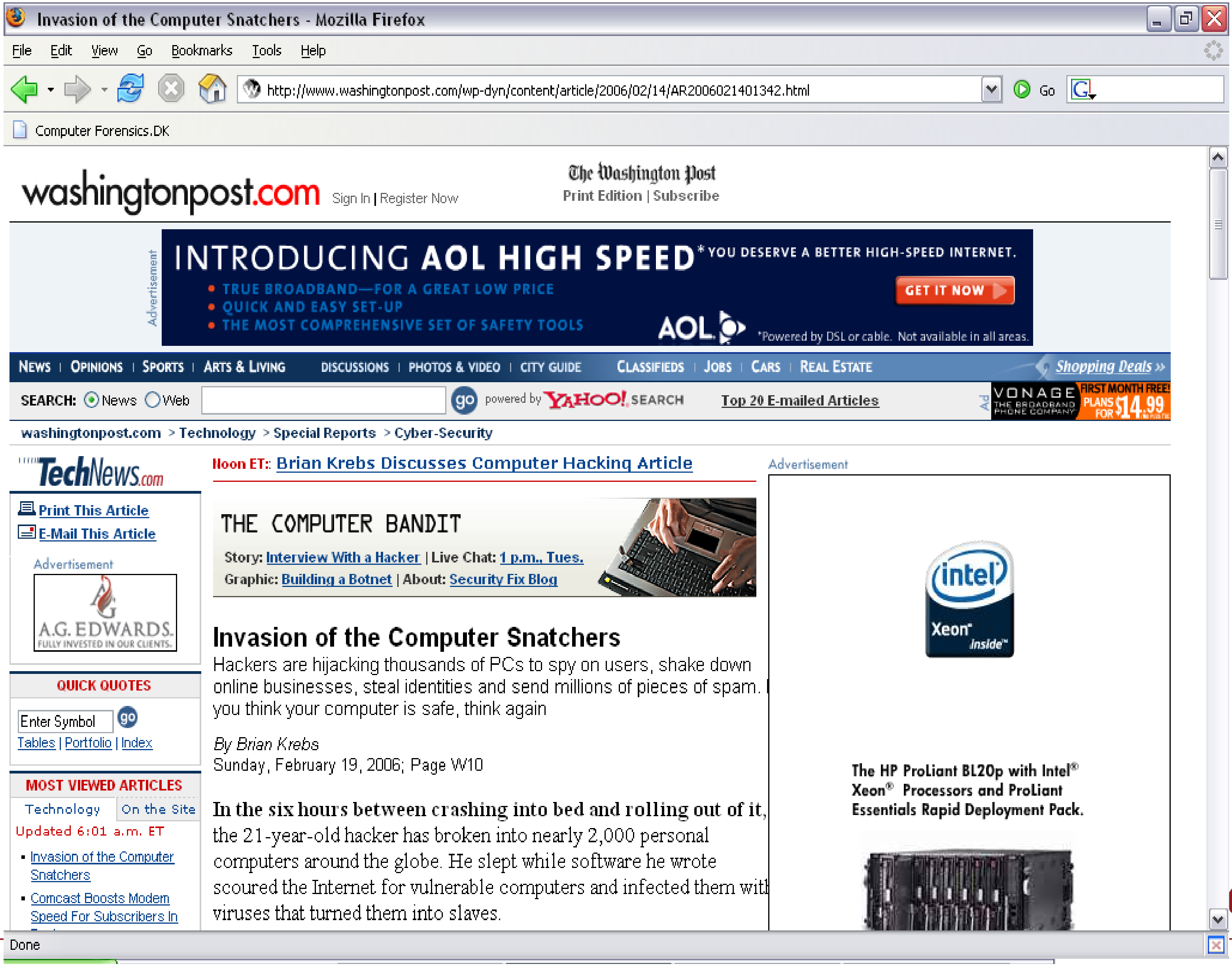
2009 © Copyright WhiteHat Security, Inc.

IT Security is difficult

Intelligent adversaries



Washington Post


Invasion of the Computer Snatchers - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
http://www.washingtonpost.com/wp-dyn/content/article/2006/02/14/AR2006021401342.html
Go
Computer Forensics.DK
washingtonpost.com Sign In | Register Now
The Washington Post
Print Edition | Subscribe
NEWS | OPINIONS | SPORTS | ARTS & LIVING DISCUSSIONS | PHOTOS & VIDEO | CITY GUIDE CLASSIFIEDS | JOBS | CARS | REAL ESTATE Shopping Deals »
SEARCH: ● News ○ Web go powered by YAHOO! SEARCH
Top 20 E-mailed Articles
washingtonpost.com > Technology > Special Reports > Cyber-Security
TechNews.com
Print This Article
E-Mail This Article
QUICK QUOTES
Enter Symbol go
Tables | Portfolio | Index
MOST VIEWED ARTICLES
Technology On the Site
Done

Noon ET: Brian Krebs Discusses Computer Hacking Article

THE COMPUTER BANDIT

Story: Interview With a Hacker | Live Chat: 1 p.m., Tues.
Graphic: Building a Botnet | About: Security Fix Blog

Updated 6:01 a.m. ET

- Invasion of the Computer Snatchers
- Comcast Boosts Modem Speed For Subscribers In

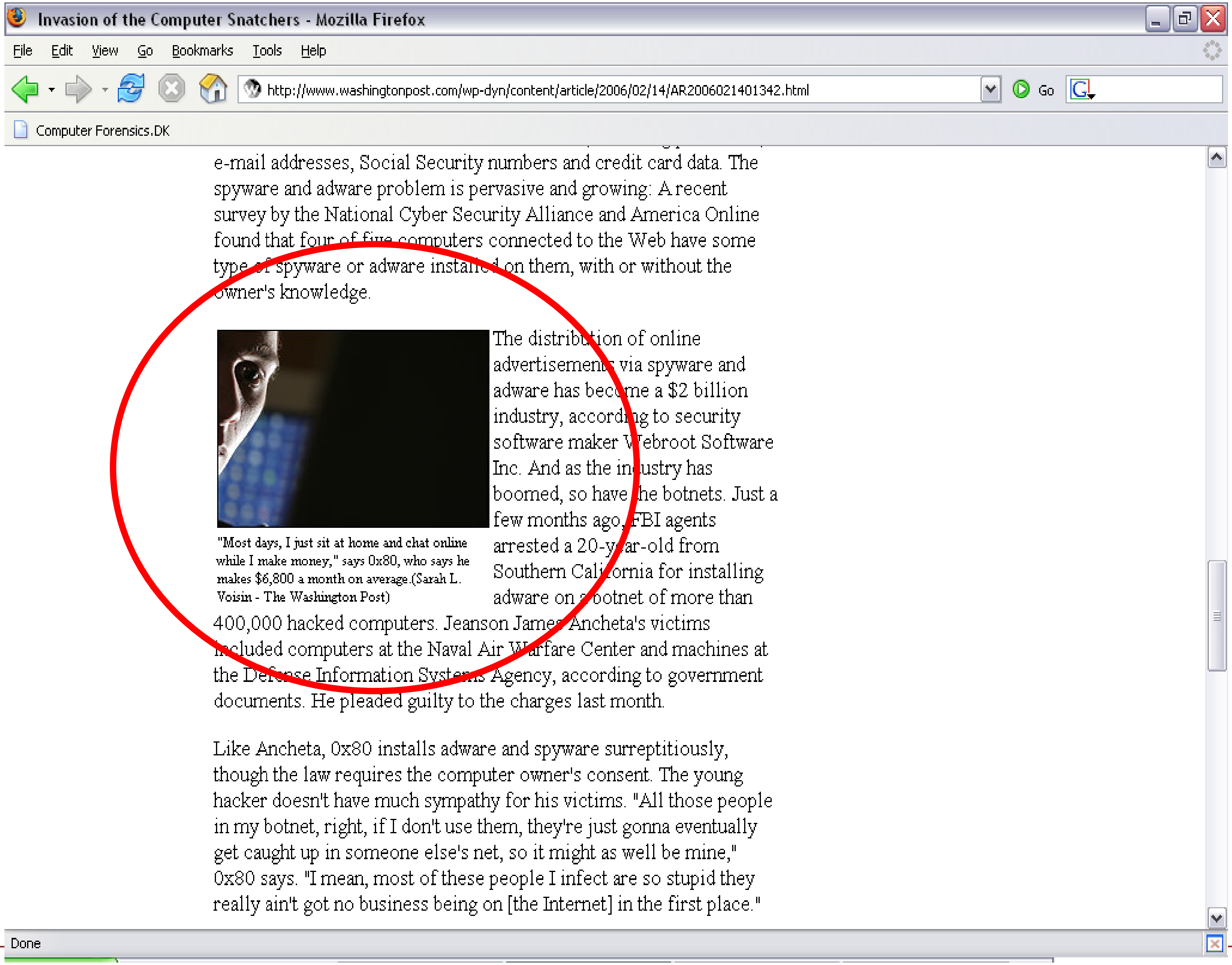
Invasion of the Computer Snatchers

Hackers are hijacking thousands of PCs to spy on users, shake down online businesses, steal identities and send millions of pieces of spam. I you think your computer is safe, think again

By Brian Krebs
Sunday, February 19, 2006; Page W10

In the six hours between crashing into bed and rolling out of it, the 21-year-old hacker has broken into nearly 2,000 personal computers around the globe. He slept while software he wrote scoured the Internet for vulnerable computers and infected them wit viruses that turned them into slaves.

Washington Post – digitale photos


Invasion of the Computer Snatchers - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
http://www.washingtonpost.com/wp-dyn/content/article/2006/02/14/AR2006021401342.html
Go
Computer Forensics.DK
Done

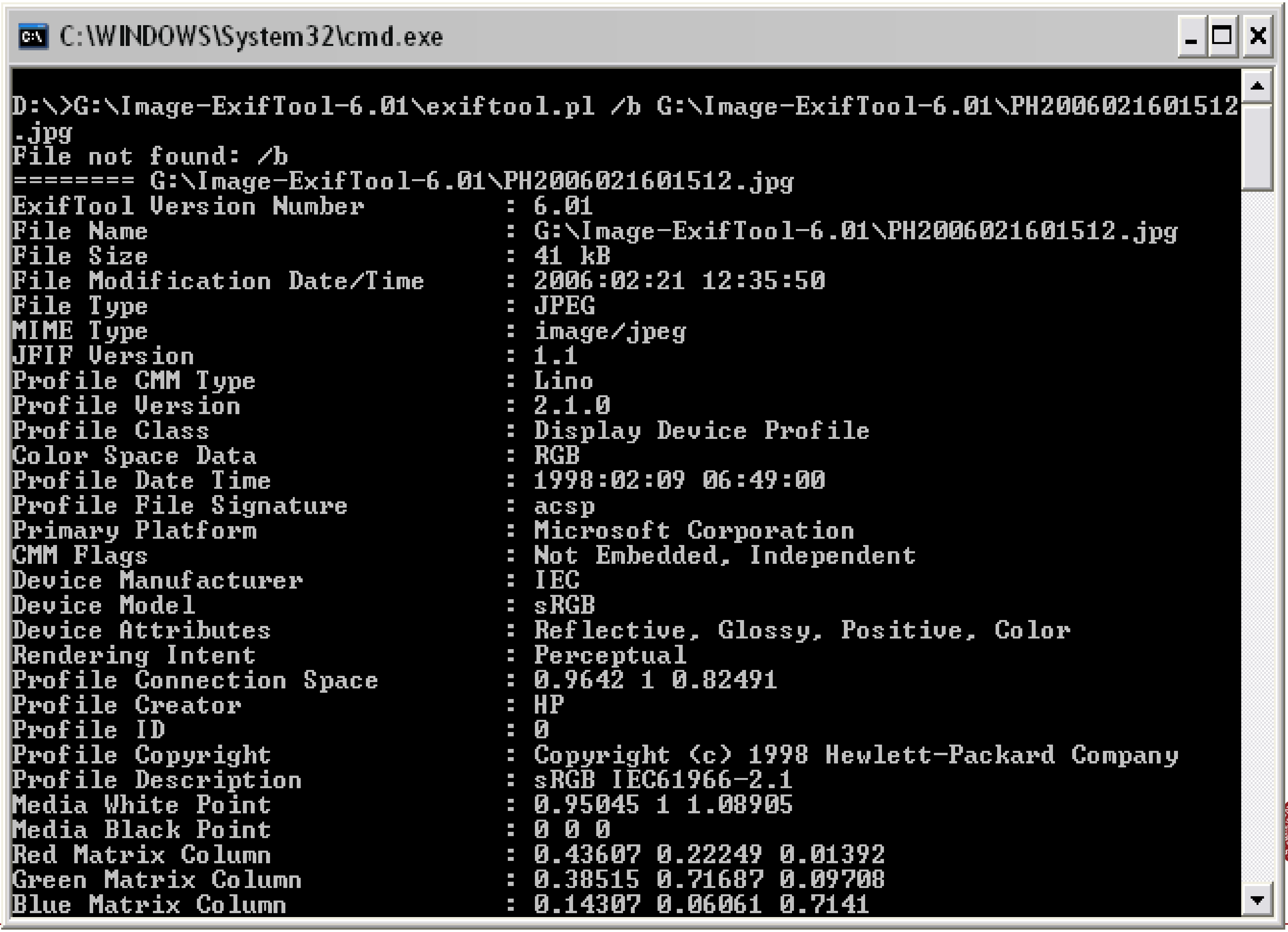
e-mail addresses, Social Security numbers and credit card data. The spyware and adware problem is pervasive and growing: A recent survey by the National Cyber Security Alliance and America Online found that four of five computers connected to the Web have some type of spyware or adware installed on them, with or without the owner's knowledge.

"Most days, I just sit at home and chat online while I make money," says 0x80, who says he makes $6,800 a month on average.(Sarah L. Voisin - The Washington Post)

The distribution of online advertisements via spyware and adware has become a $2 billion industry, according to security software maker Webroot Software Inc. And as the industry has boomed, so have the botnets. Just a few months ago, FBI agents arrested a 20-year-old from Southern California for installing adware on a botnet of more than 400,000 hacked computers. Jeanson James Ancheta's victims included computers at the Naval Air Warfare Center and machines at the Defense Information Systems Agency, according to government documents. He pleaded guilty to the charges last month.

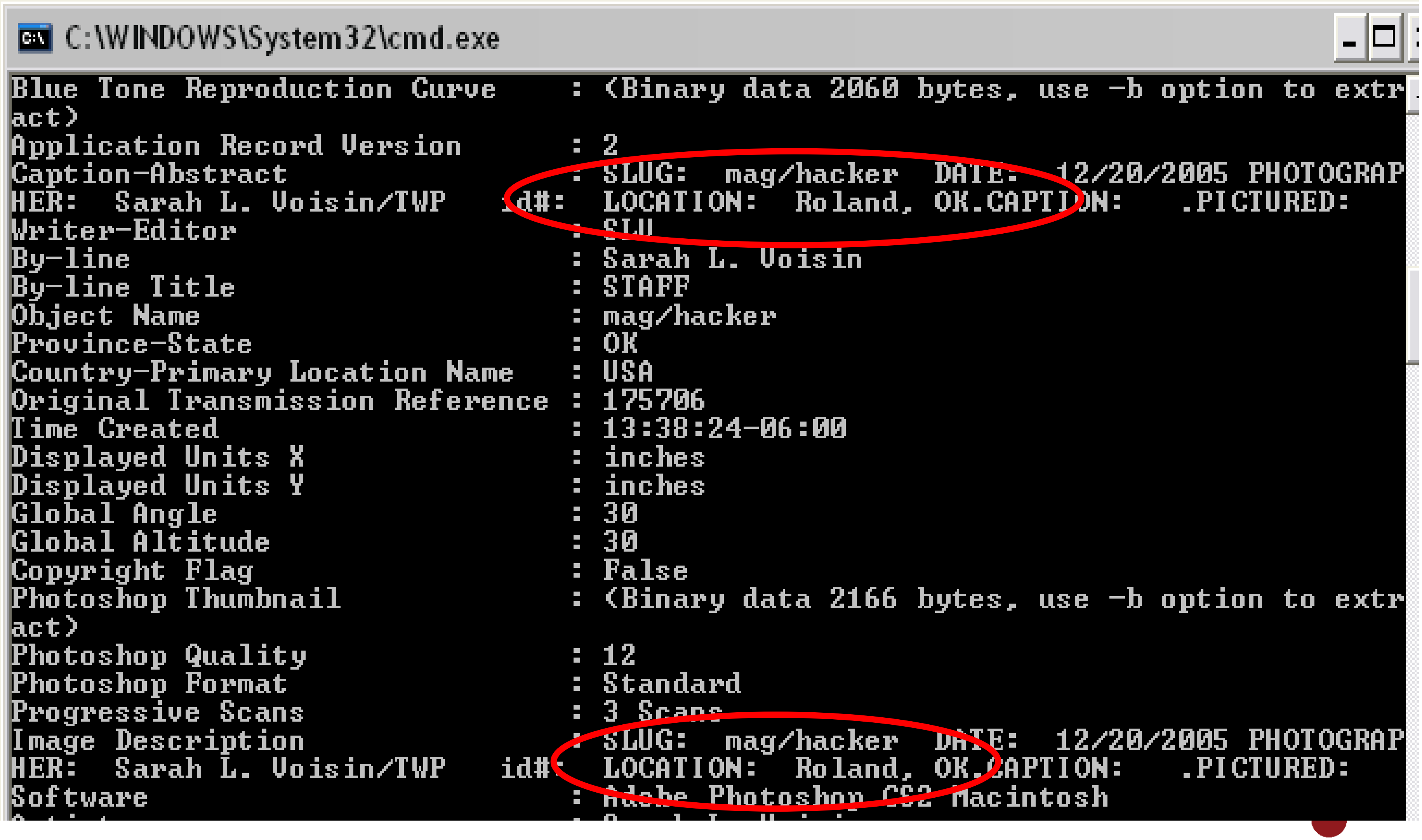
Like Ancheta, 0x80 installs adware and spyware surreptitiously, though the law requires the computer owner's consent. The young hacker doesn't have much sympathy for his victims. "All those people in my botnet, right, if I don't use them, they're just gonna eventually get caught up in someone else's net, so it might as well be mine," 0x80 says. "I mean, most of these people I infect are so stupid they really ain't got no business being on [the Internet] in the first place."

Washington Post – digitale photos



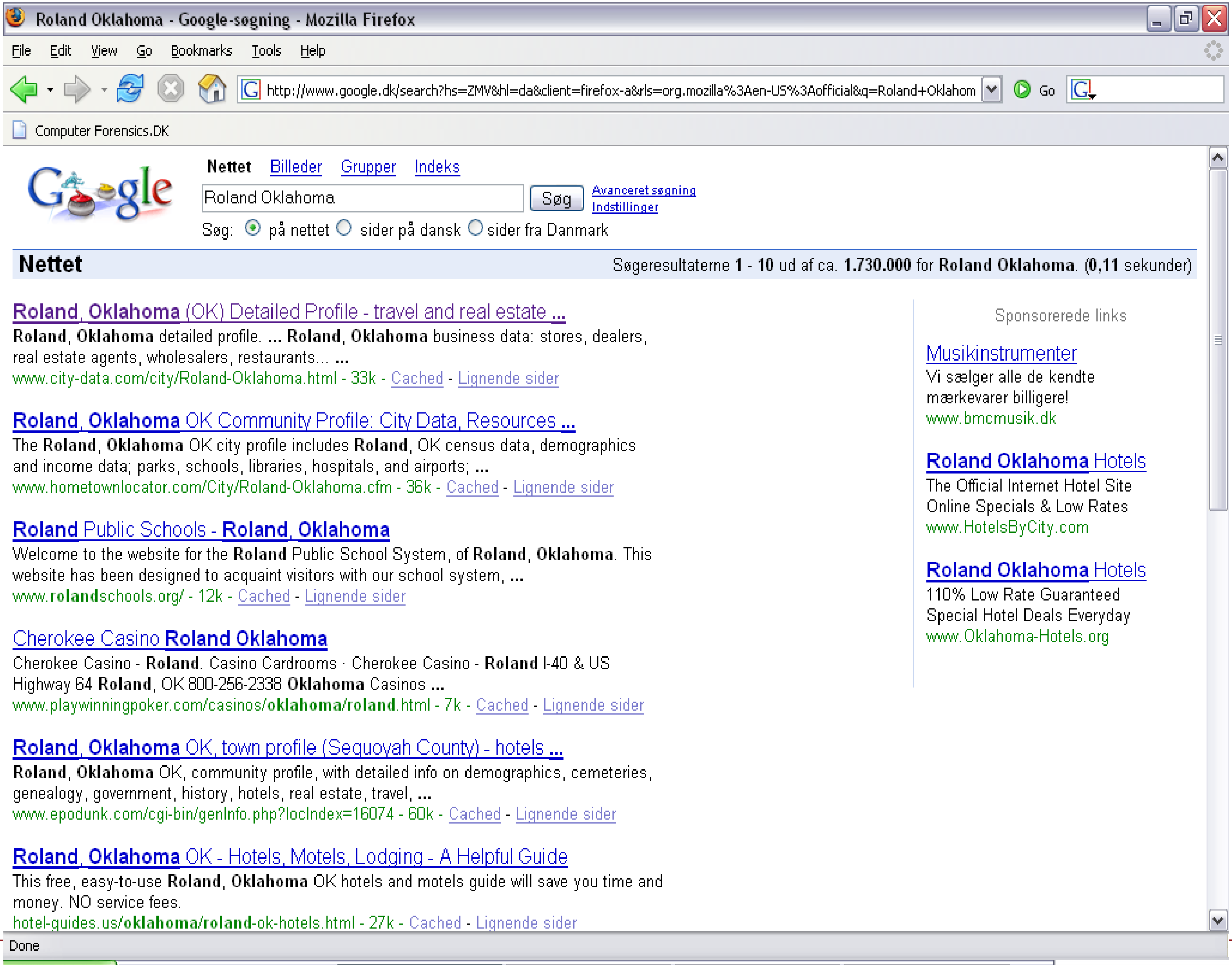
```
D:\>G:\Image-ExifTool-6.01\exiftool.pl /b G:\Image-ExifTool-6.01\PH2006021601512
.jpg
File not found: /b
======== G:\Image-ExifTool-6.01\PH2006021601512.jpg
ExifTool Version Number         : 6.01
File Name                       : G:\Image-ExifTool-6.01\PH2006021601512.jpg
File Size                       : 41 kB
File Modification Date/Time     : 2006:02:21 12:35:50
File Type                       : JPEG
MIME Type                       : image/jpeg
JFIF Version                    : 1.1
Profile CMM Type                : Lino
Profile Version                 : 2.1.0
Profile Class                   : Display Device Profile
Color Space Data                : RGB
Profile Date Time               : 1998:02:09 06:49:00
Profile File Signature          : acsp
Primary Platform                : Microsoft Corporation
CMM Flags                       : Not Embedded, Independent
Device Manufacturer             : IEC
Device Model                    : sRGB
Device Attributes               : Reflective, Glossy, Positive, Color
Rendering Intent                : Perceptual
Profile Connection Space        : 0.9642 1 0.82491
Profile Creator                 : HP
Profile ID                      : 0
Profile Copyright               : Copyright (c) 1998 Hewlett-Packard Company
Profile Description             : sRGB IEC61966-2.1
Media White Point               : 0.95045 1 1.08905
Media Black Point               : 0 0 0
Red Matrix Column               : 0.43607 0.22249 0.01392
Green Matrix Column             : 0.38515 0.71687 0.09708
Blue Matrix Column              : 0.14307 0.06061 0.7141
```

Washington Post – digitale photos



```
Blue Tone Reproduction Curve      : (Binary data 2060 bytes, use -b option to extr
act)
Application Record Version        : 2
Caption-Abstract                  : SLUG:  mag/hacker  DATE:  12/20/2005 PHOTOGRAP
HER:  Sarah L. Voisin/TWP   id#:  LOCATION:  Roland, OK.CAPTION:   .PICTURED:
Writer-Editor                     : SLU
By-line                           : Sarah L. Voisin
By-line Title                     : STAFF
Object Name                       : mag/hacker
Province-State                    : OK
Country-Primary Location Name     : USA
Original Transmission Reference   : 175706
Time Created                      : 13:38:24-06:00
Displayed Units X                 : inches
Displayed Units Y                 : inches
Global Angle                      : 30
Global Altitude                   : 30
Copyright Flag                    : False
Photoshop Thumbnail               : (Binary data 2166 bytes, use -b option to extr
act)
Photoshop Quality                 : 12
Photoshop Format                  : Standard
Progressive Scans                 : 3 Scans
Image Description                 : SLUG:  mag/hacker  DATE:  12/20/2005 PHOTOGRAP
HER:  Sarah L. Voisin/TWP   id#:  LOCATION:  Roland, OK.CAPTION:   .PICTURED:
Software                          : Adobe Photoshop CS2 Macintosh
```

Washington Post – Google



http://www.google.dk/search?hs=ZMV&hl=da&client=firefox-a&rls=org.mozilla%3Aen-US%3Aofficial&q=Roland+Oklahom

Roland Oklahoma

Søg: ● på nettet ○ sider på dansk ○ sider fra Danmark

Nettet Søgeresultaterne **1** - **10** ud af ca. **1.730.000** for **Roland Oklahoma**. (**0,11** sekunder)

Roland, **Oklahoma** (OK) Detailed Profile - travel and real estate ...
Roland, **Oklahoma** detailed profile. ... **Roland**, **Oklahoma** business data: stores, dealers, real estate agents, wholesalers, restaurants... ...
www.city-data.com/city/Roland-Oklahoma.html - 33k - Cached - Lignende sider

Roland, **Oklahoma** OK Community Profile: City Data, Resources ...
The **Roland**, **Oklahoma** OK city profile includes **Roland**, OK census data, demographics and income data; parks, schools, libraries, hospitals, and airports; ...
www.hometownlocator.com/City/Roland-Oklahoma.cfm - 36k - Cached - Lignende sider

Roland Public Schools - **Roland**, **Oklahoma**
Welcome to the website for the **Roland** Public School System, of **Roland**, **Oklahoma**. This website has been designed to acquaint visitors with our school system, ...
www.**roland**schools.org/ - 12k - Cached - Lignende sider

Cherokee Casino **Roland Oklahoma**
Cherokee Casino - **Roland**. Casino Cardrooms · Cherokee Casino - **Roland** I-40 & US Highway 64 **Roland**, OK 800-256-2338 **Oklahoma** Casinos ...
www.playwinningpoker.com/casinos/**oklahoma**/**roland**.html - 7k - Cached - Lignende sider

Roland, **Oklahoma** OK, town profile (Sequoyah County) - hotels ...
Roland, **Oklahoma** OK, community profile, with detailed info on demographics, cemeteries, genealogy, government, history, hotels, real estate, travel, ...
www.epodunk.com/cgi-bin/genInfo.php?locIndex=16074 - 60k - Cached - Lignende sider

Roland, **Oklahoma** OK - Hotels, Motels, Lodging - A Helpful Guide
This free, easy-to-use **Roland**, **Oklahoma** OK hotels and motels guide will save you time and money. NO service fees.
hotel-guides.us/**oklahoma**/**roland**-ok-hotels.html - 27k - Cached - Lignende sider

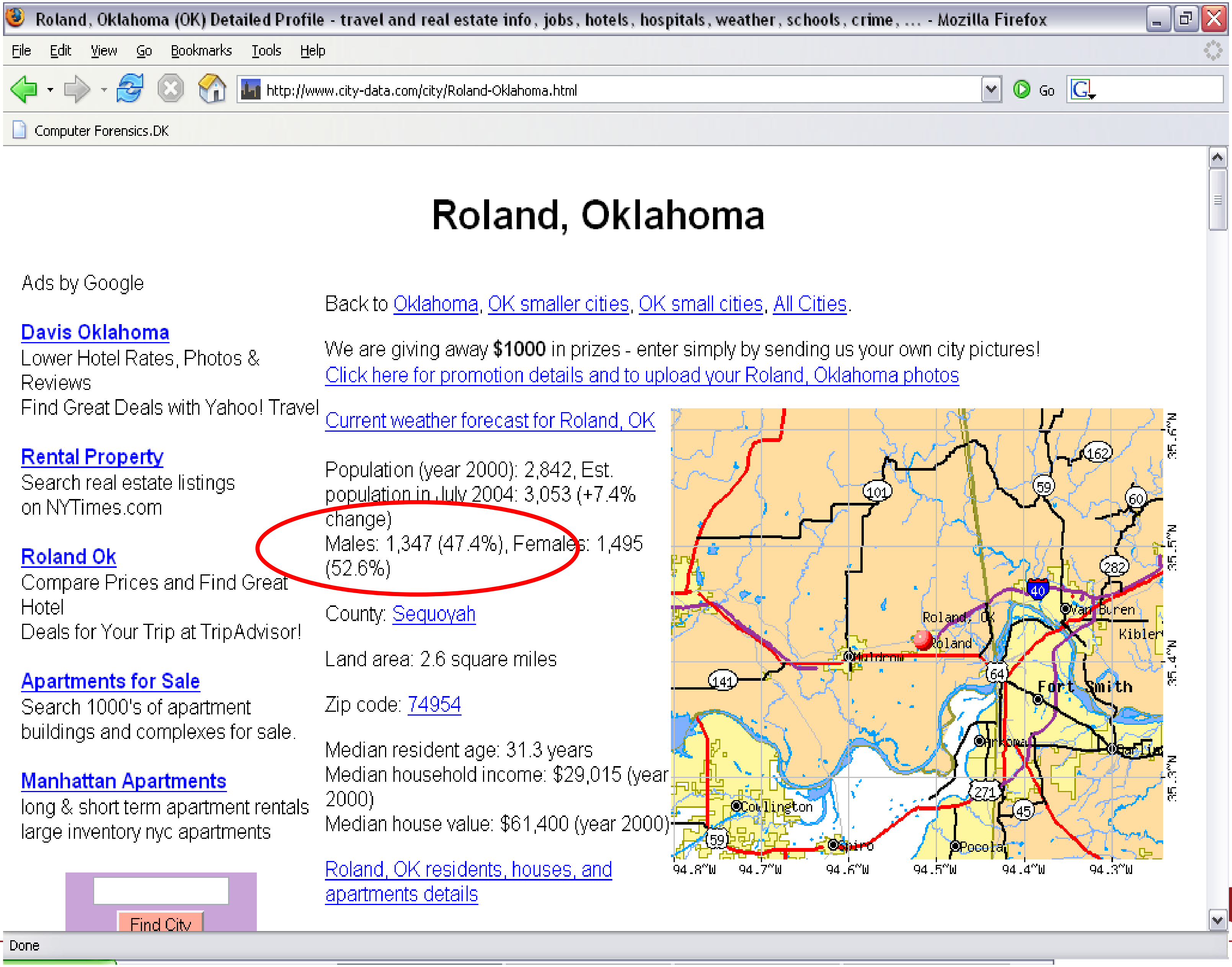
Sponsorerede links

Musikinstrumenter
Vi sælger alle de kendte mærkevarer billigere!
www.bmcmusik.dk

Roland Oklahoma Hotels
The Official Internet Hotel Site
Online Specials & Low Rates
www.HotelsByCity.com

Roland Oklahoma Hotels
110% Low Rate Guaranteed
Special Hotel Deals Everyday
www.Oklahoma-Hotels.org

Washington Post – Google



Roland, Oklahoma (OK) Detailed Profile - travel and real estate info, jobs, hotels, hospitals, weather, schools, crime, ... - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
http://www.city-data.com/city/Roland-Oklahoma.html
Go
Computer Forensics.DK
Done

Roland, Oklahoma

Find City

Back to Oklahoma, OK smaller cities, OK small cities, All Cities.

We are giving away **$1000** in prizes - enter simply by sending us your own city pictures!
Click here for promotion details and to upload your Roland, Oklahoma photos

Current weather forecast for Roland, OK

Population (year 2000): 2,842, Est. population in July 2004: 3,053 (+7.4% change)
Males: 1,347 (47.4%), Females: 1,495 (52.6%)

County: Sequoyah

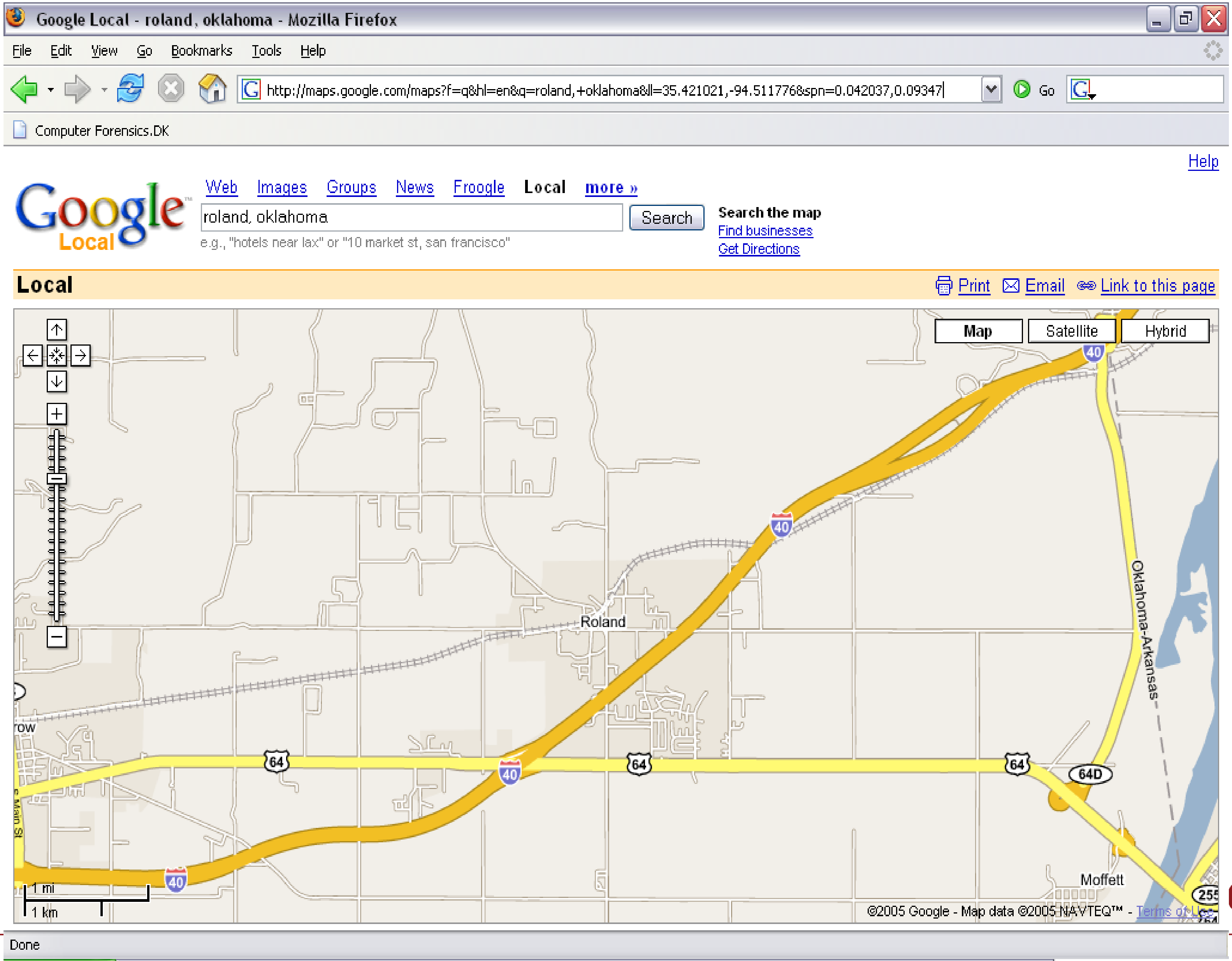
Land area: 2.6 square miles

Zip code: 74954

Median resident age: 31.3 years
Median household income: $29,015 (year 2000)
Median house value: $61,400 (year 2000)

Roland, OK residents, houses, and apartments details

Washington Post – Google



Google Local - roland, oklahoma - Mozilla Firefox

http://maps.google.com/maps?f=q&hl=en&q=roland,+oklahoma&ll=35.421021,-94.511776&spn=0.042037,0.09347

roland, oklahoma

e.g., "hotels near lax" or "10 market st, san francisco"

©2005 Google - Map data ©2005 NAVTEQ™ - Terms of Use

Done

Who is the hackeren?

- Lives in Roland, Oklahoma (1347 men in town)

From the article:
- 21 years old
- High school dropout.
- Blond hair, covers the eyebrows
- Skinny ("wiry frame", "tall and lanky")
- Smokes cigarettes. (Marlboros, probably Marlboro Light)
- Lives with parents in a "brick rambler"
- Have a dog ("A small dog with matted fur")

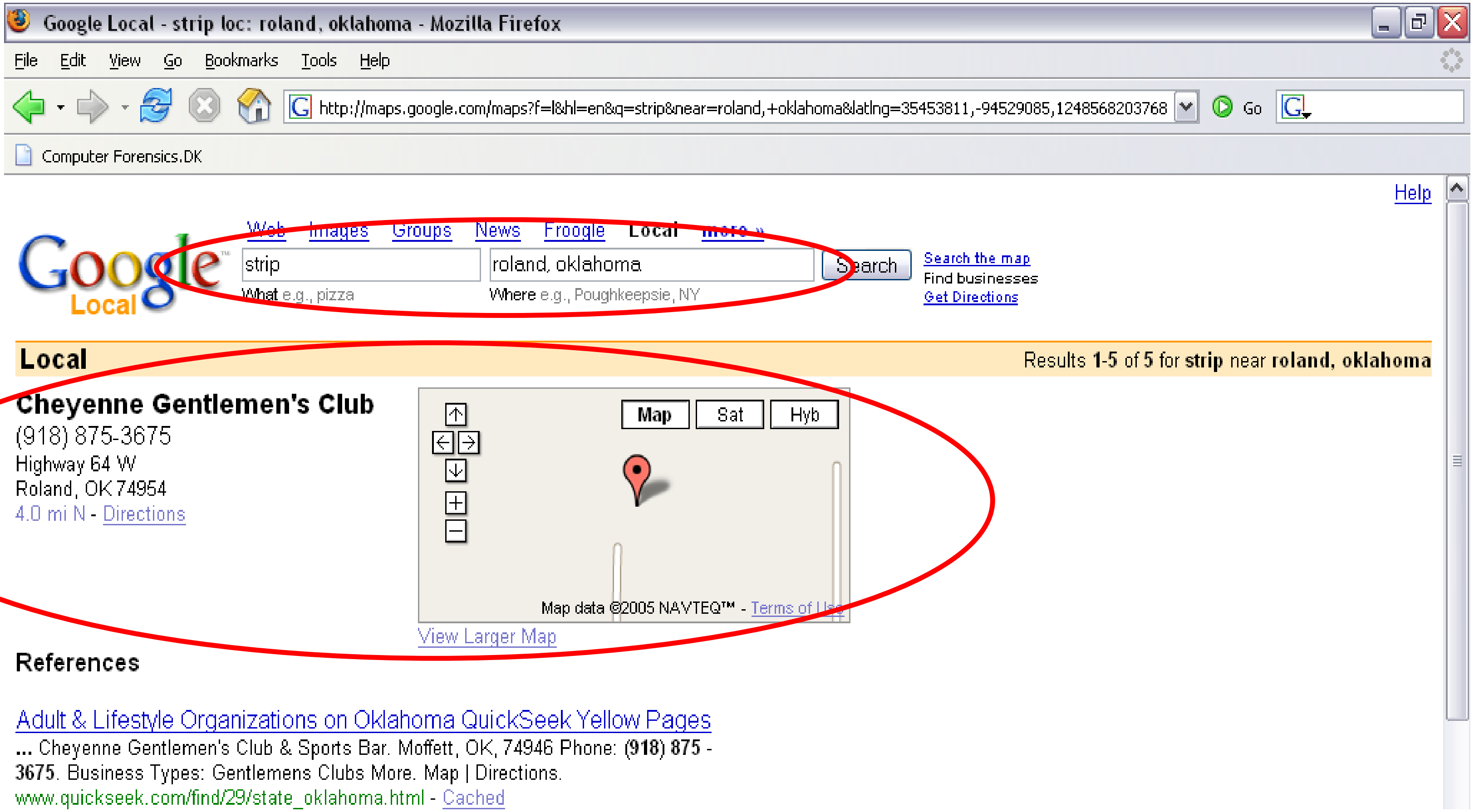
Washington Post – more info from the article

“He lives with his folks in a small town in Middle America. The nearest businesses are a used-car lot, a gas station/convenience store and a strip club, where 0x80 says he recently dropped $800 for an hour alone in a VIP room with several dancers.“

Washington Post – more info from the article

“He lives with his folks in a small town in Middle America. The nearest businesses are a used-car lot, a gas station/convenience store and a strip club, where 0x80 says he recently dropped $800 for an hour alone in a VIP room with several dancers.“

Washington Post – Google



http://maps.google.com/maps?f=l&hl=en&q=strip&near=roland,+oklahoma&latlng=35453811,-94529085,1248568203768

What: strip (e.g., pizza)

Where: roland, oklahoma (e.g., Poughkeepsie, NY)

Search the map
Find businesses
Get Directions

Local Results **1-5** of **5** for **strip** near **roland, oklahoma**

Cheyenne Gentlemen's Club
(918) 875-3675
Highway 64 W
Roland, OK 74954
4.0 mi N - Directions

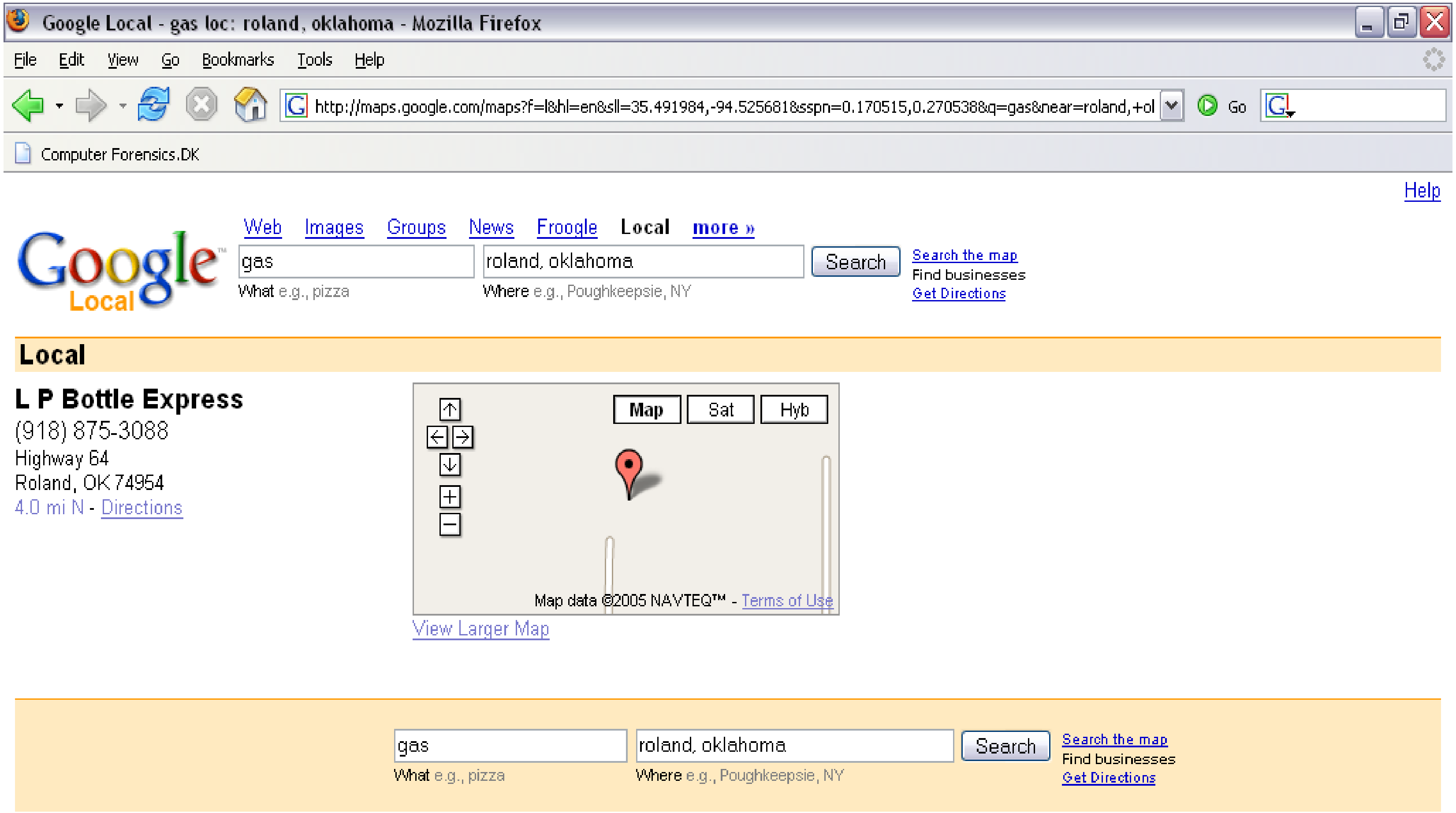
Map data ©2005 NAVTEQ™ - Terms of Use

View Larger Map

References

Adult & Lifestyle Organizations on Oklahoma QuickSeek Yellow Pages
... Cheyenne Gentlemen's Club & Sports Bar. Moffett, OK, 74946 Phone: **(918) 875** - **3675**. Business Types: Gentlemens Clubs More. Map | Directions.
www.quickseek.com/find/29/state_oklahoma.html - Cached

Washington Post – Google



Google Local - gas loc: roland, oklahoma - Mozilla Firefox

http://maps.google.com/maps?f=l&hl=en&sll=35.491984,-94.525681&sspn=0.170515,0.270538&q=gas&near=roland,+ol

Computer Forensics.DK

What: gas

Where: roland, oklahoma

Local

L P Bottle Express
(918) 875-3088
Highway 64
Roland, OK 74954
4.0 mi N - Directions

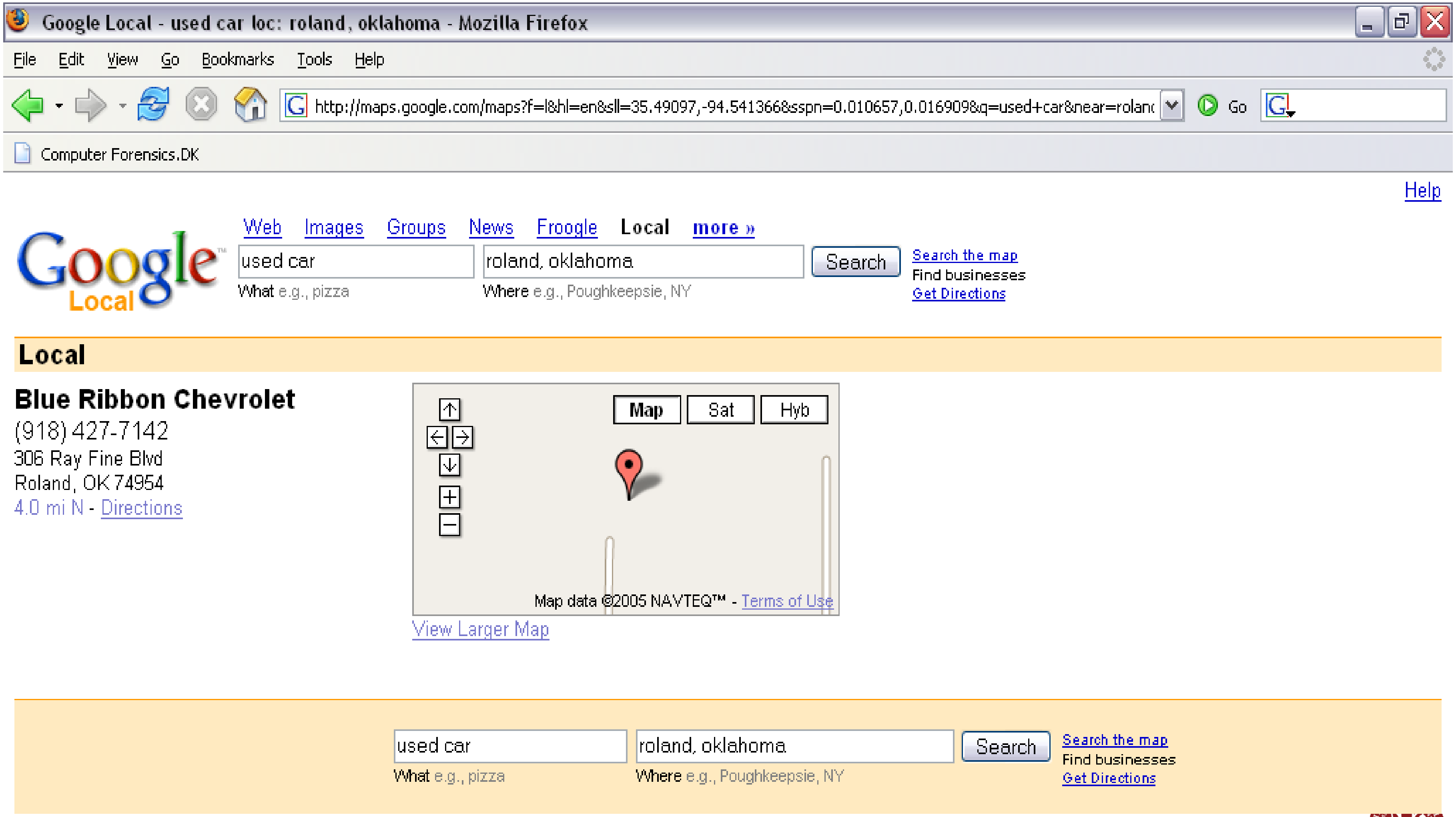
Map data ©2005 NAVTEQ™ - Terms of Use

View Larger Map

What: gas

Where: roland, oklahoma

Washington Post – Google



Google Local - used car loc: roland, oklahoma - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
Go
Computer Forensics.DK
Help
Web Images Groups News Froogle Local more »
Google Local
Search
Search the map
Find businesses
Get Directions
Map Sat Hyb
View Larger Map

http://maps.google.com/maps?f=l&hl=en&sll=35.49097,-94.5413668sspn=0.010657,0.0169098q=used+car&near=rolanc

What: used car e.g., pizza

Where: roland, oklahoma e.g., Poughkeepsie, NY

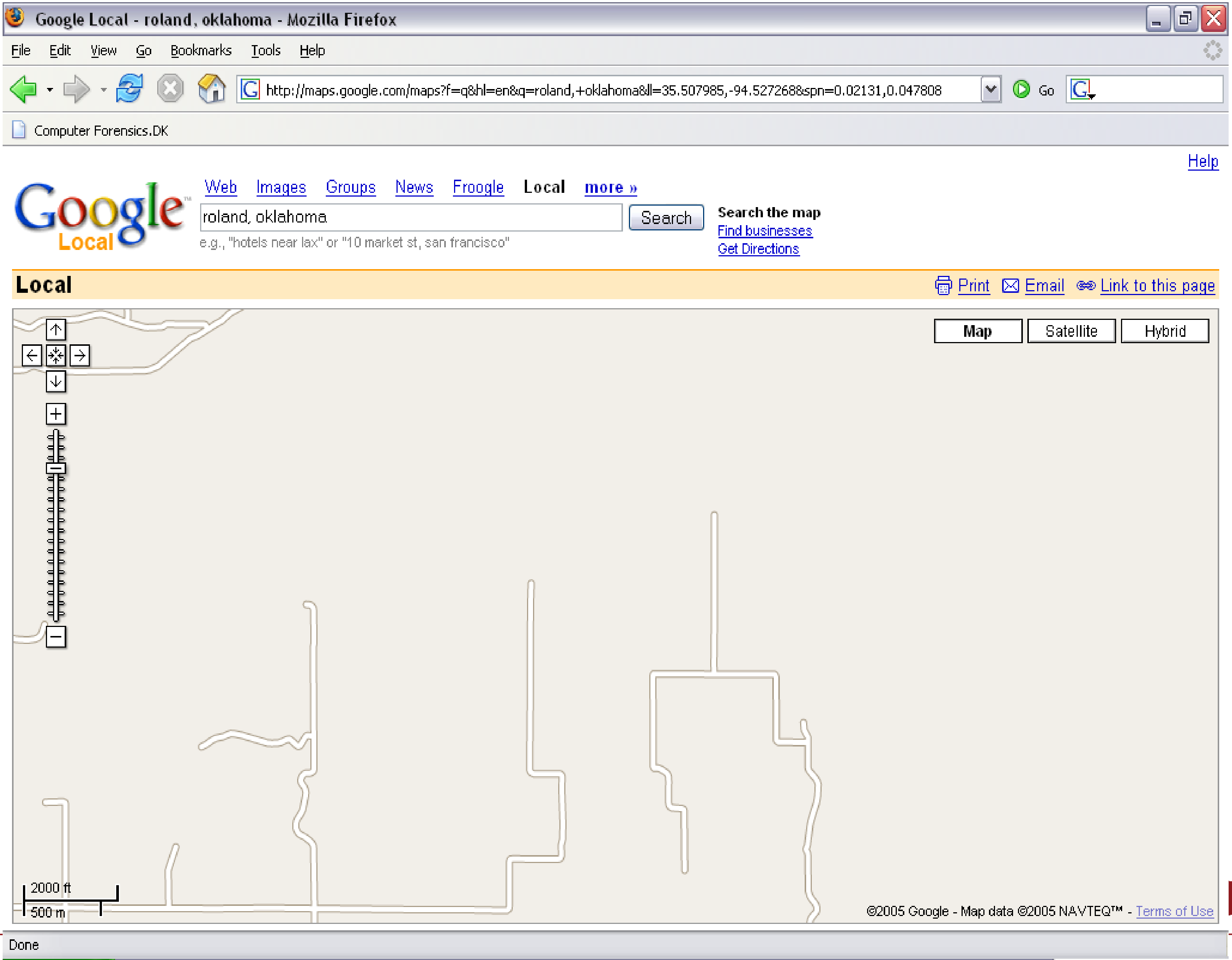
Local

Blue Ribbon Chevrolet
(918) 427-7142
306 Ray Fine Blvd
Roland, OK 74954
4.0 mi N - Directions

Map data ©2005 NAVTEQ™ - Terms of Use

What: used car e.g., pizza

Where: roland, oklahoma e.g., Poughkeepsie, NY



Google Local - roland, oklahoma - Mozilla Firefox

http://maps.google.com/maps?f=q&hl=en&q=roland,+oklahoma&ll=35.507985,-94.527268&spn=0.02131,0.047808

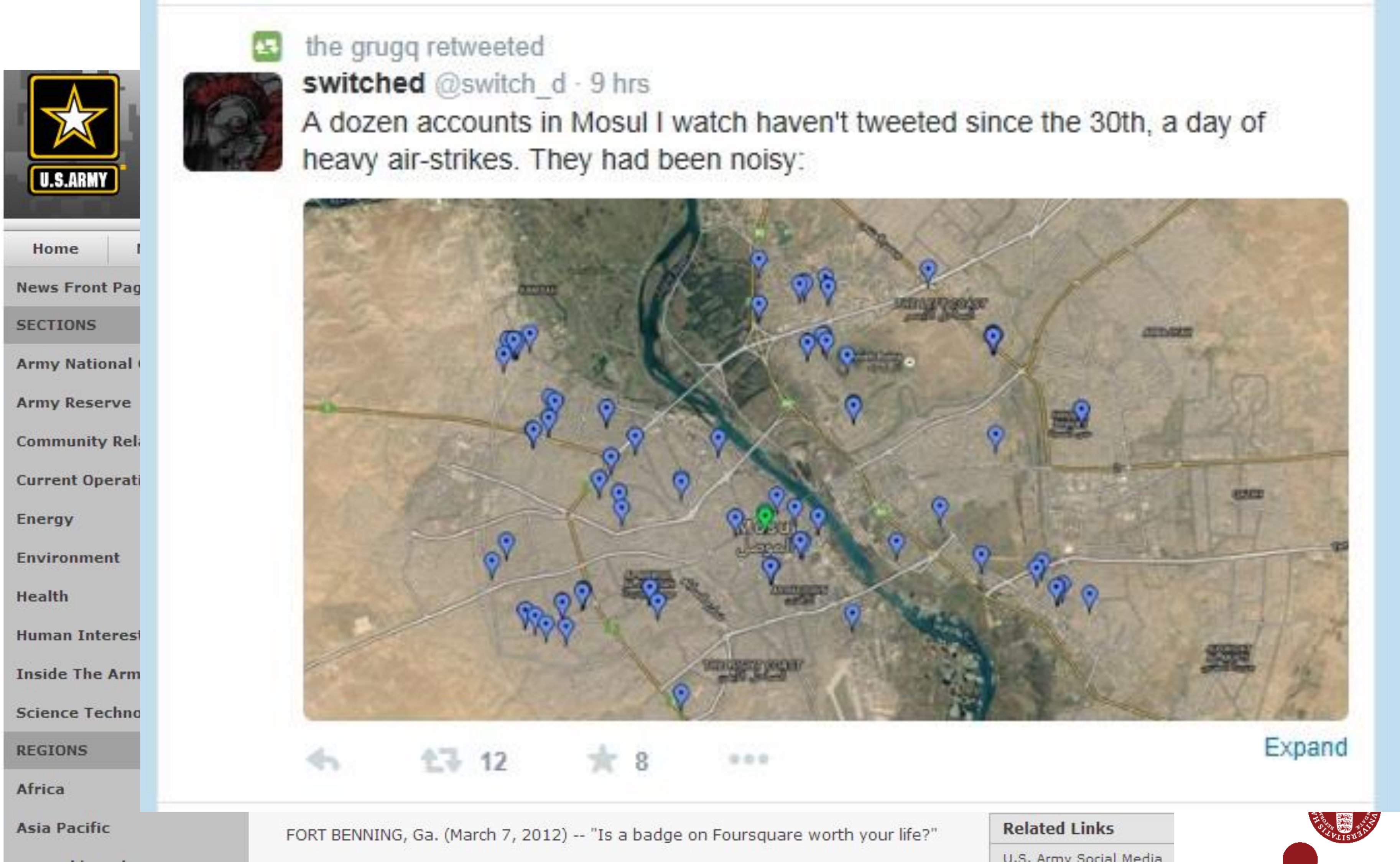
roland, oklahoma

e.g., "hotels near lax" or "10 market st, san francisco"

©2005 Google - Map data ©2005 NAVTEQ™ - Terms of Use

Done

Metadata and bombs



the grugq retweeted

switched @switch_d · 9 hrs

A dozen accounts in Mosul I watch haven't tweeted since the 30th, a day of heavy air-strikes. They had been noisy:

Home

News Front Pag

SECTIONS

Army National

Army Reserve

Community Rel

Current Operati

Energy

Environment

Health

Human Interest

Inside The Arm

Science Techno

REGIONS

Africa

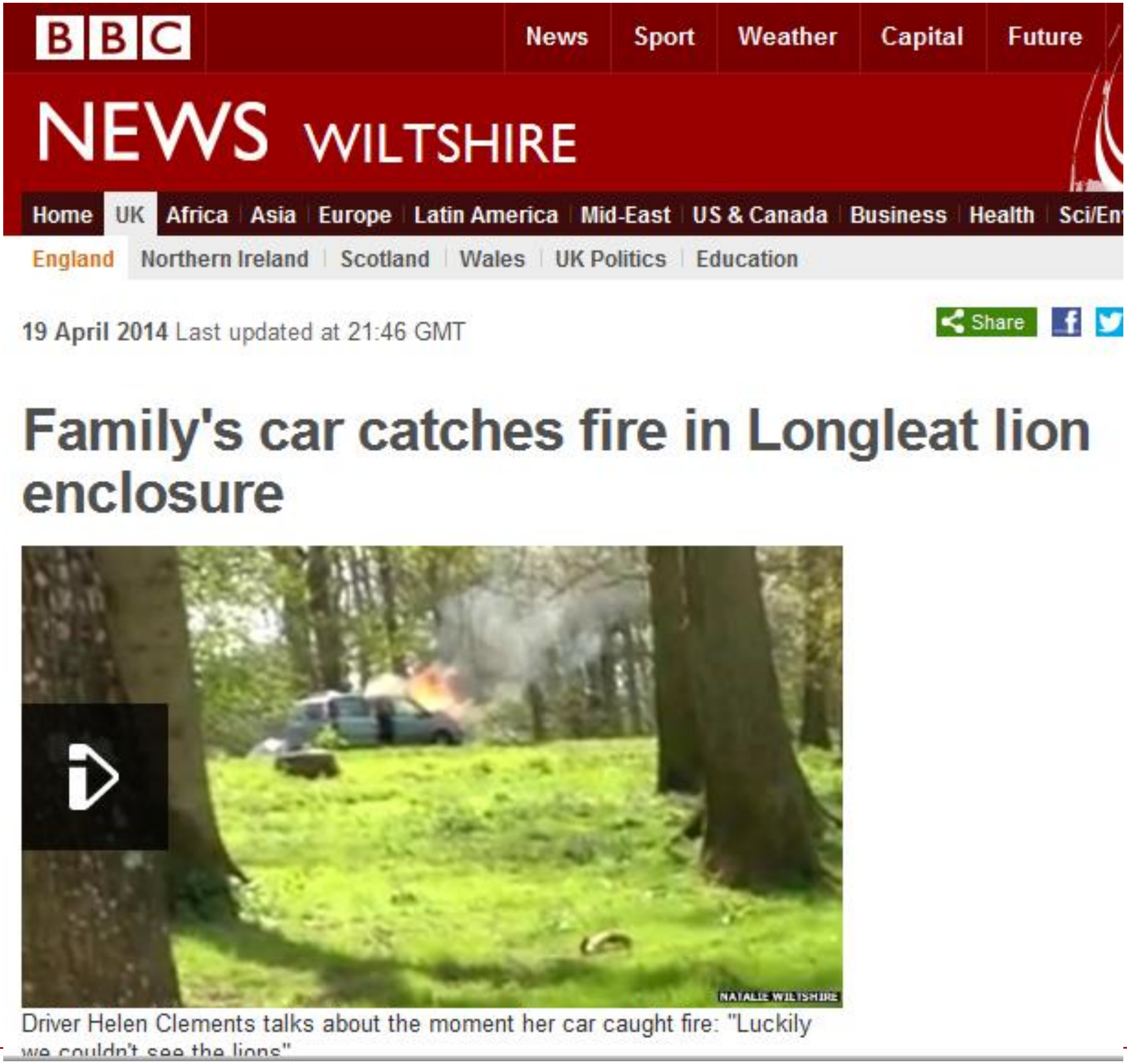
Asia Pacific

FORT BENNING, Ga. (March 7, 2012) -- "Is a badge on Foursquare worth your life?"

Related Links

U.S. Army Social Media

Hard to assess all relevant threats



19 April 2014 Last updated at 21:46 GMT

Family's car catches fire in Longleat lion enclosure

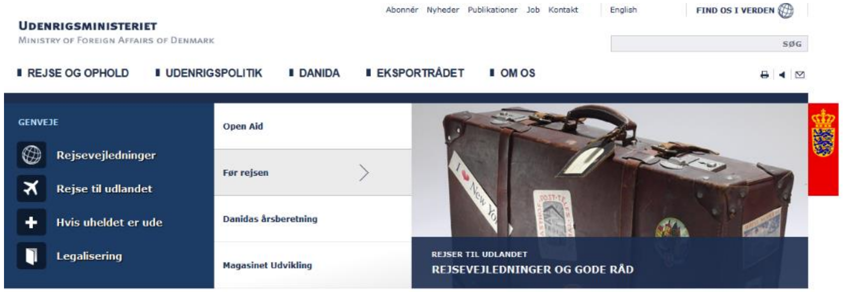
Driver Helen Clements talks about the moment her car caught fire: "Luckily we couldn't see the lions"

Which is "Best"?

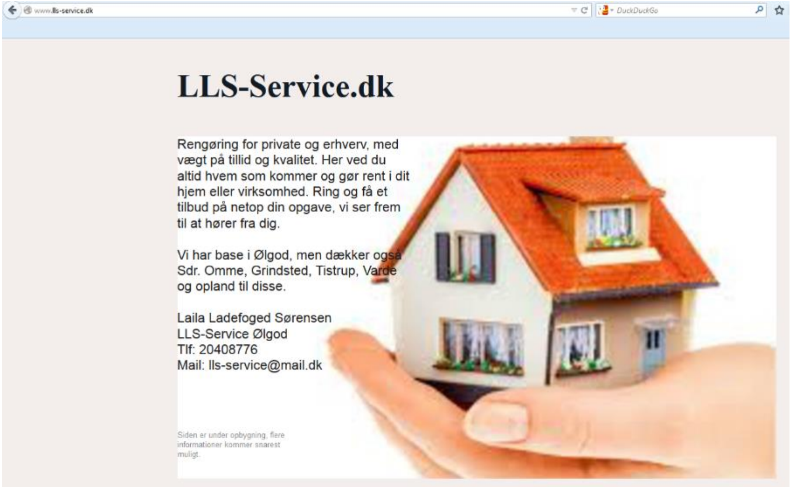
Part of the herd – or a target?

VS

Part of the herd – or a target?



LLS-Service.dk



LLS-Service.dk

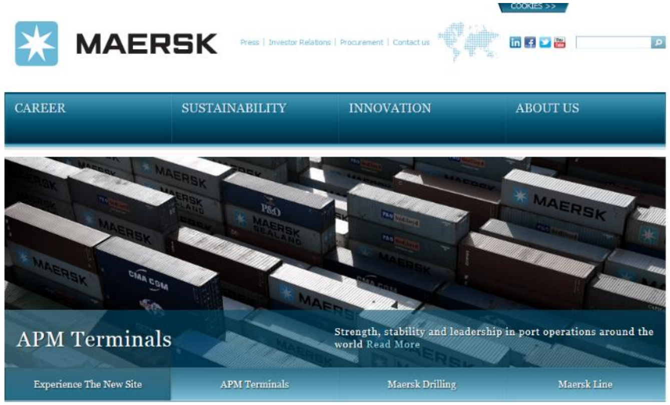
Rengøring for private og erhverv, med vægt på tillid og kvalitet. Her ved du altid hvem som kommer og gør rent i dit hjem eller virksomhed. Ring og få et tilbud på netop din opgave, vi ser frem til at hører fra dig.

Vi har base i Ølgod, men dækker også Sdr. Omme, Grindsted, Tistrup, Varde og opland til disse.

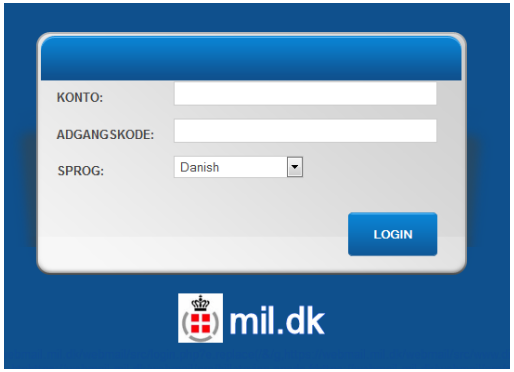
Laila Ladefoged Sørensen
LLS-Service Ølgod
Tlf: 20408776
Mail: lls-service@mail.dk

Siden er under opbygning, flere informationer kommer snarest muligt.

VS



Strength, stability and leadership in port operations around the world Read More



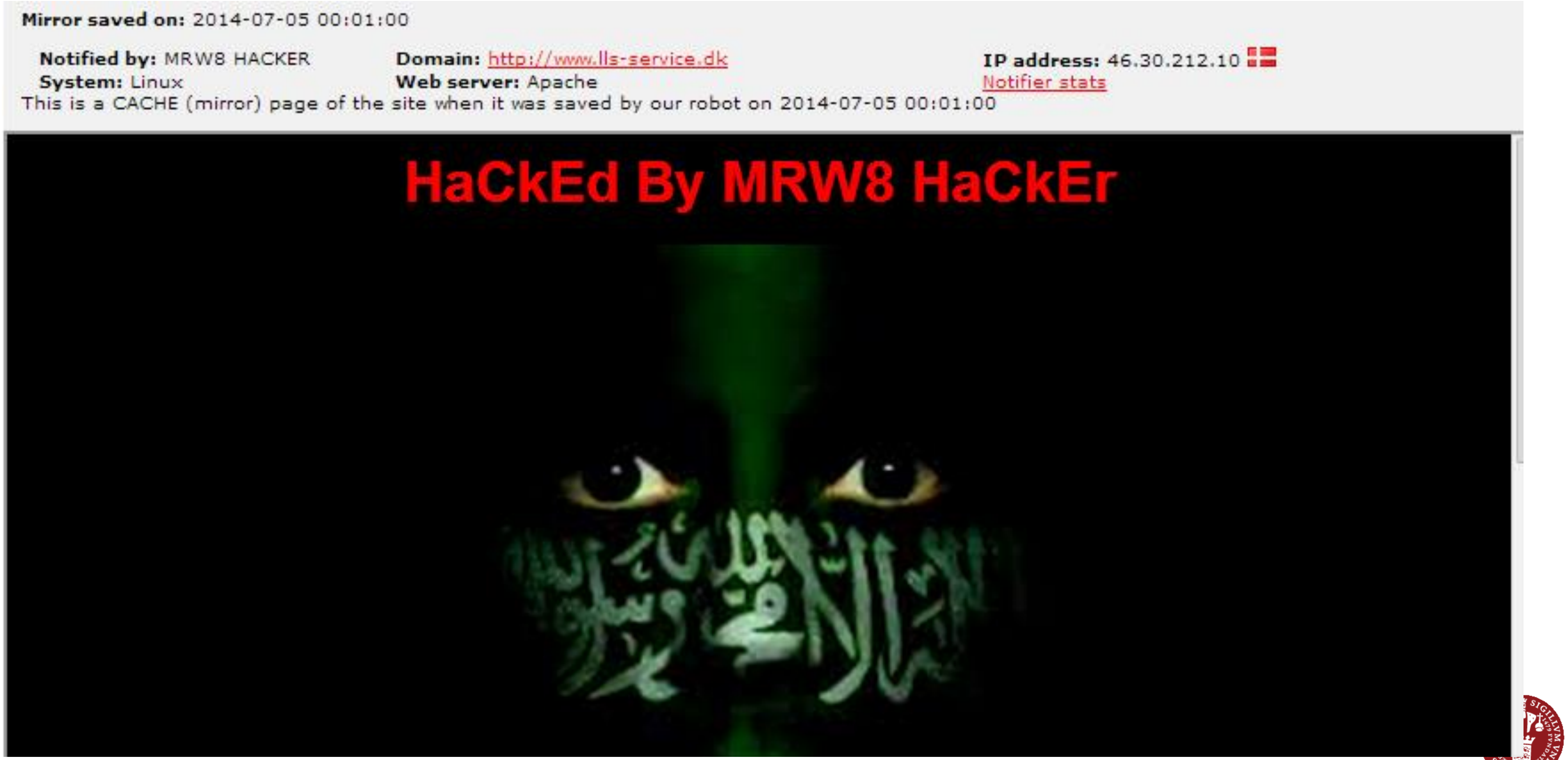
KONTO:

ADGANGSKODE:

SPROG: Danish

Part of the herd – can still get hit

LLS-Service.dk



Mirror saved on: 2014-07-05 00:01:00

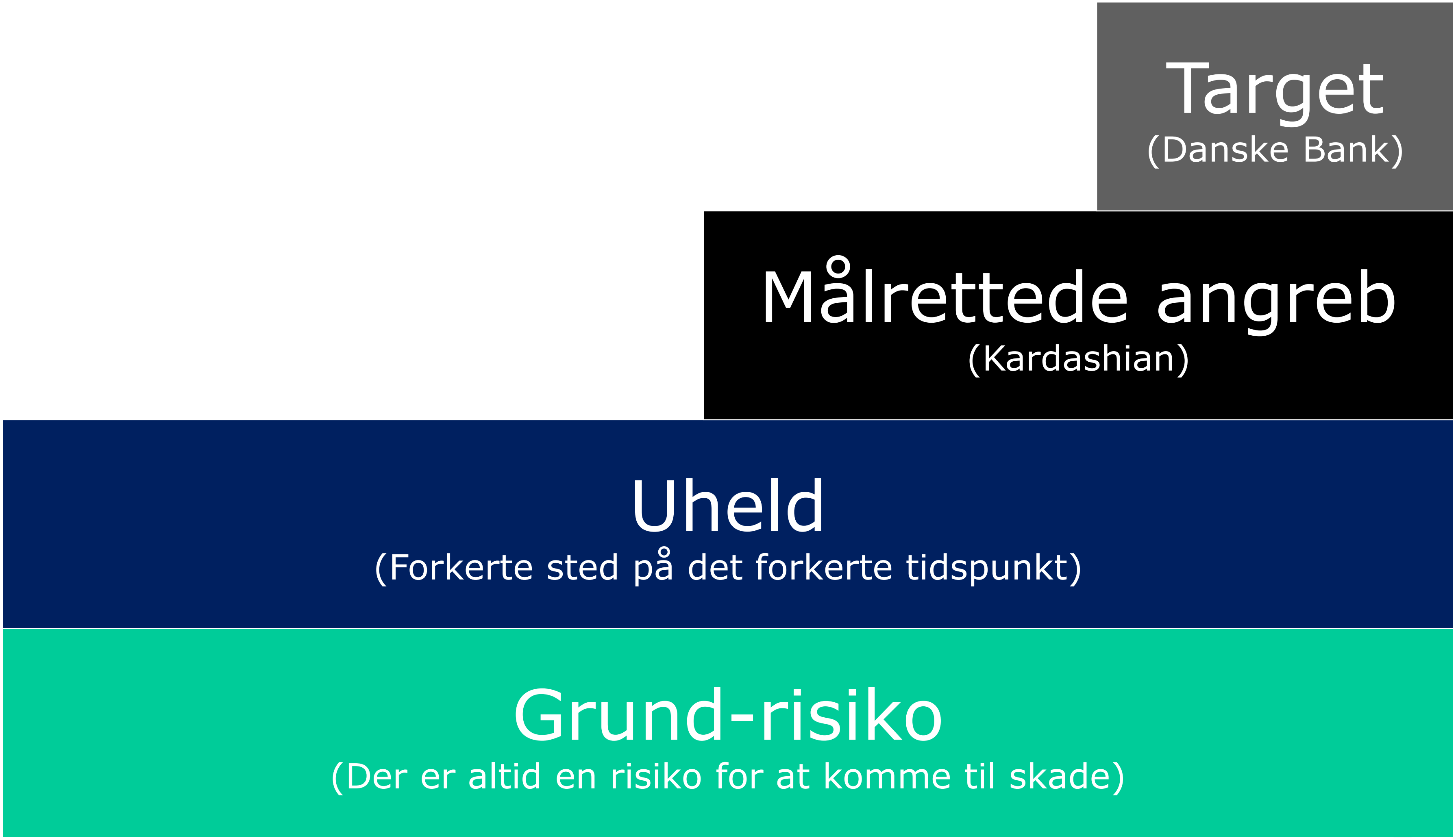
Notified by: MRW8 HACKER **Domain:** http://www.lls-service.dk **IP address:** 46.30.212.10

System: Linux **Web server:** Apache Notifier stats

This is a CACHE (mirror) page of the site when it was saved by our robot on 2014-07-05 00:01:00

HaCkEd By MRW8 HaCkEr

What assets are we trying to protect?



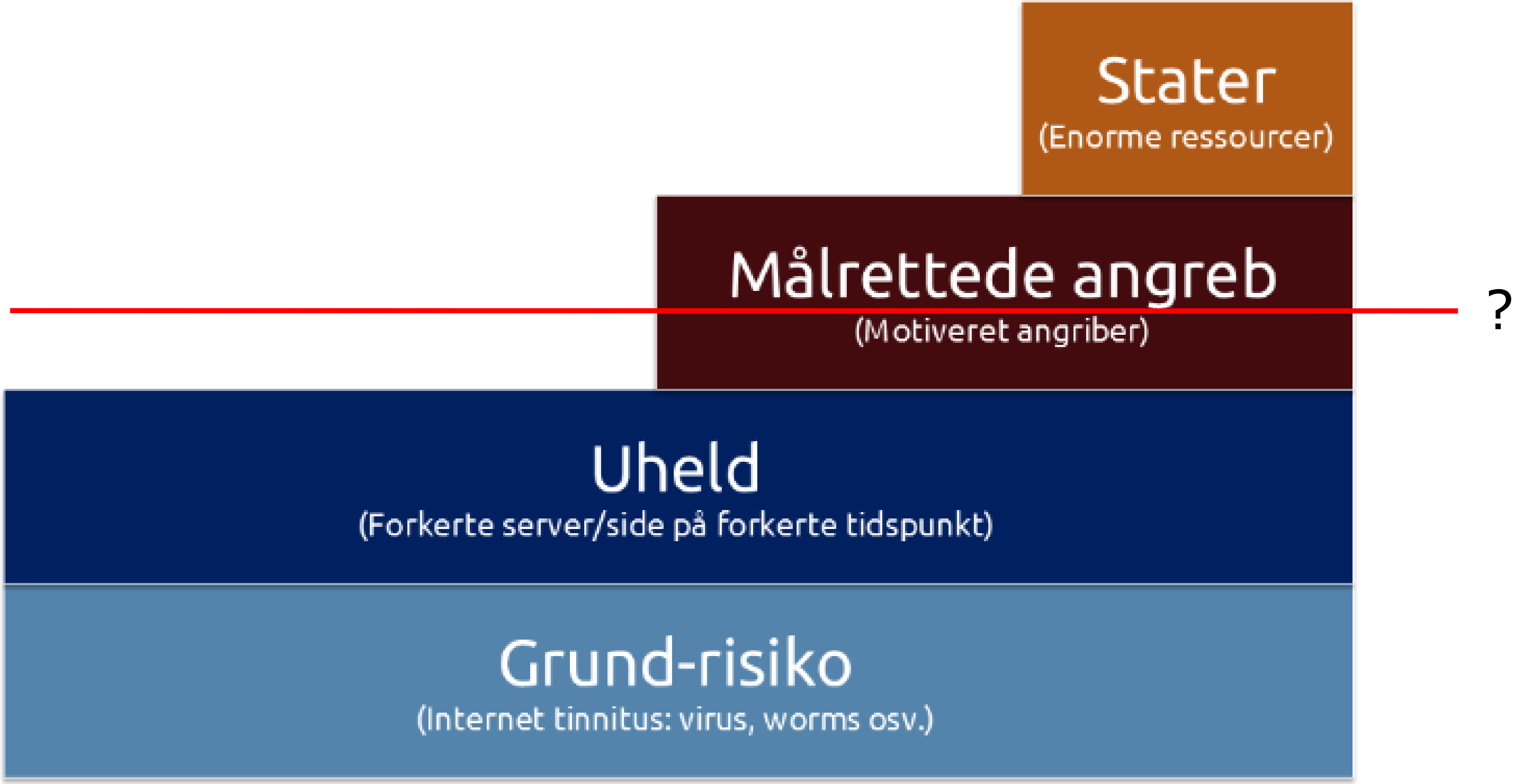
Target
(Danske Bank)

Målrettede angreb
(Kardashian)

Uheld
(Forkerte sted på det forkerte tidspunkt)

Grund-risiko
(Der er altid en risiko for at komme til skade)

Where should you put the bar?


Stater
(Enorme ressourcer)

Målrettede angreb
(Motiveret angriber)

?

Uheld
(Forkerte server/side på forkerte tidspunkt)

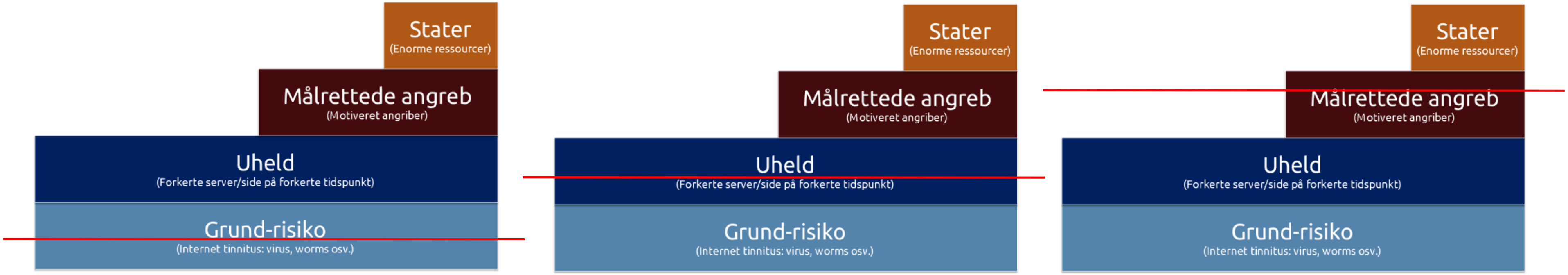
Grund-risiko
(Internet tinnitus: virus, worms osv.)

Risk appetite

Risk appetite varies (a lot)

Risk appetite (risiko villighed):

Startup, manufacturer, bank >< consequence



Stater
(Enorme ressourcer)

Målrettede angreb
(Motiveret angriber)

Uheld
(Forkerte server/side på forkerte tidspunkt)

Grund-risiko
(Internet tinnitus: virus, worms osv.)

Start-up

Stater
(Enorme ressourcer)

Målrettede angreb
(Motiveret angriber)

Uheld
(Forkerte server/side på forkerte tidspunkt)

Grund-risiko
(Internet tinnitus: virus, worms osv.)

Produktionsvirksomhed

Stater
(Enorme ressourcer)

Målrettede angreb
(Motiveret angriber)

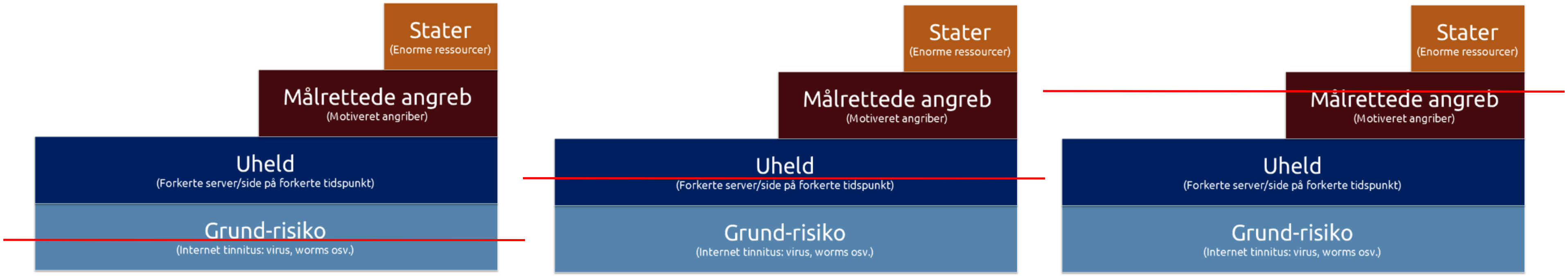
Uheld
(Forkerte server/side på forkerte tidspunkt)

Grund-risiko
(Internet tinnitus: virus, worms osv.)

Bank/Mærsk/[UM/militæret]

One of the main problems…

It is difficult to really access the consequence



Stater
(Enorme ressourcer)

Målrettede angreb
(Motiveret angriber)

Uheld
(Forkerte server/side på forkerte tidspunkt)

Grund-risiko
(Internet tinnitus: virus, worms osv.)

Stater
(Enorme ressourcer)

Målrettede angreb
(Motiveret angriber)

Uheld
(Forkerte server/side på forkerte tidspunkt)

Grund-risiko
(Internet tinnitus: virus, worms osv.)

Stater
(Enorme ressourcer)

Målrettede angreb
(Motiveret angriber)

Uheld
(Forkerte server/side på forkerte tidspunkt)

Grund-risiko
(Internet tinnitus: virus, worms osv.)

Start-up

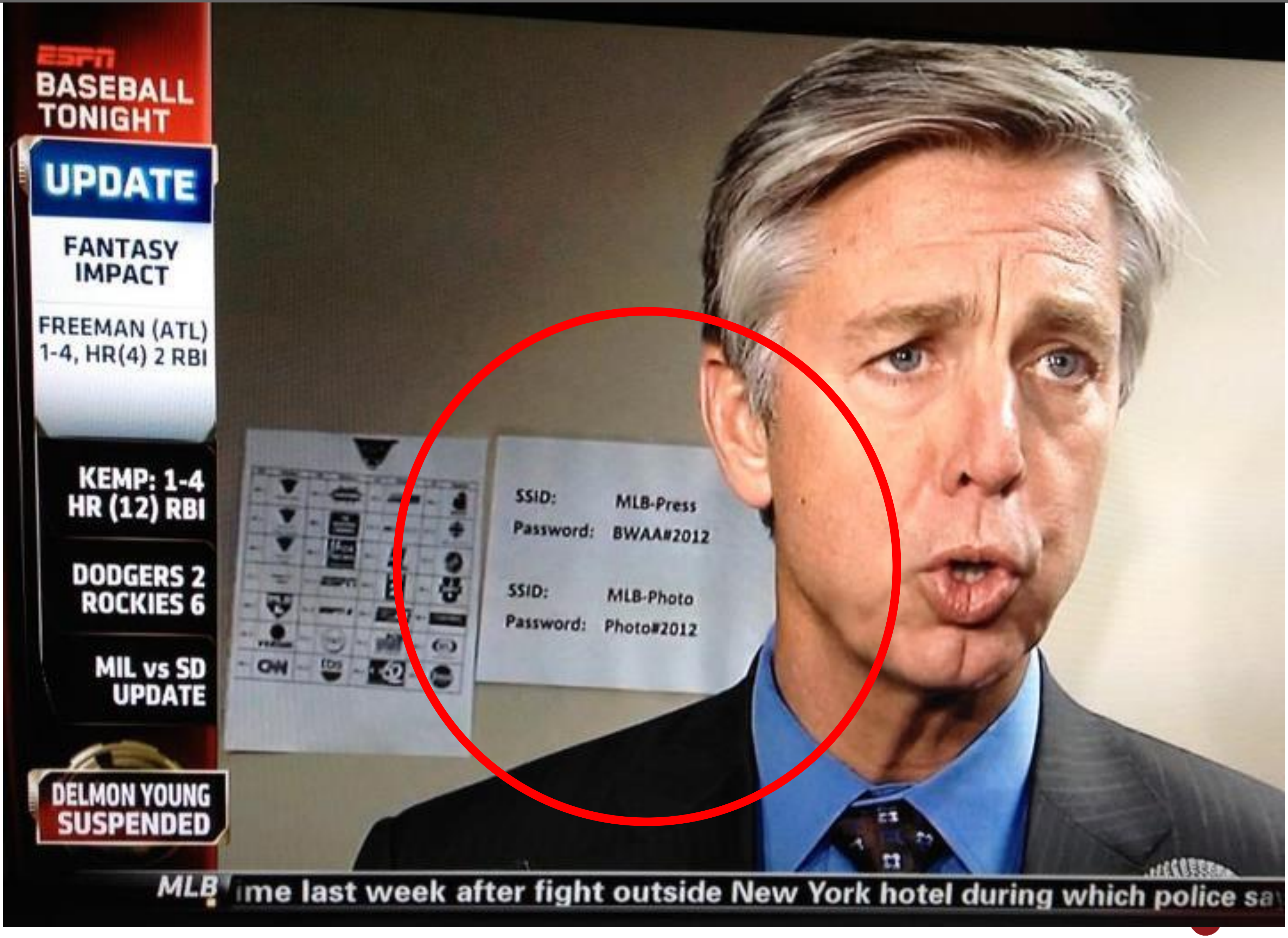
Produktionsvirksomhed

Bank/Mærsk/[UM/militæret]

Hard to assess all relevant threats correctly

Everyone has soap in their shower, and yet so few people slip to their death in the morning!
Dave Aitel

”What’s possible” vs. ”What’s probable”



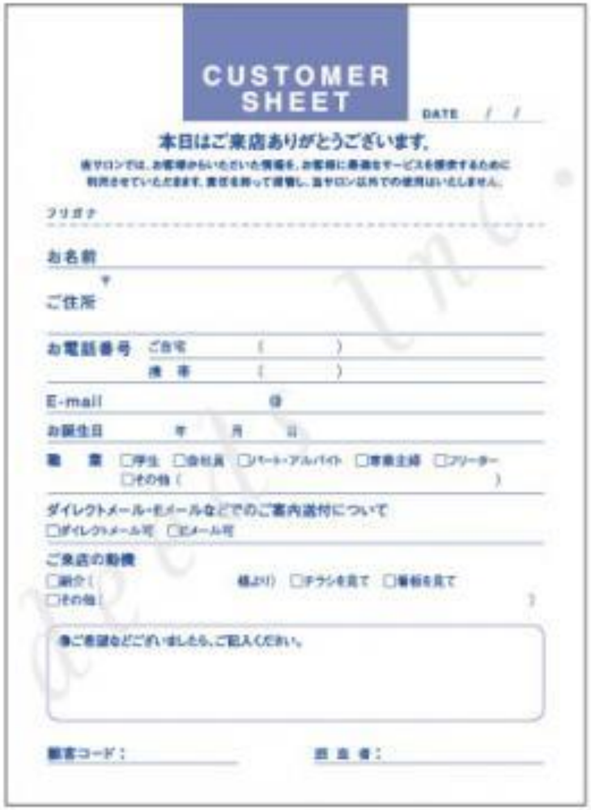
SSID: MLB-Press
Password: BWAA#2012

SSID: MLB-Photo
Password: Photo#2012

Security analysis

Threats, risks and consequences

A security solution



CUSTOMER SHEET

DATE　/　/

本日はご来店ありがとうございます。

当サロンでは、お客様からいただいた情報を、お客様に最適なサービスを提供するために利用させていただきます。責任を持って保管し、当サロン以外での使用はいたしません。

フリガナ

お名前

〒

ご住所

お電話番号　ご自宅　（　　）
　　　　　　携　帯　（　　）

E-mail　　@

お誕生日　　年　月　日

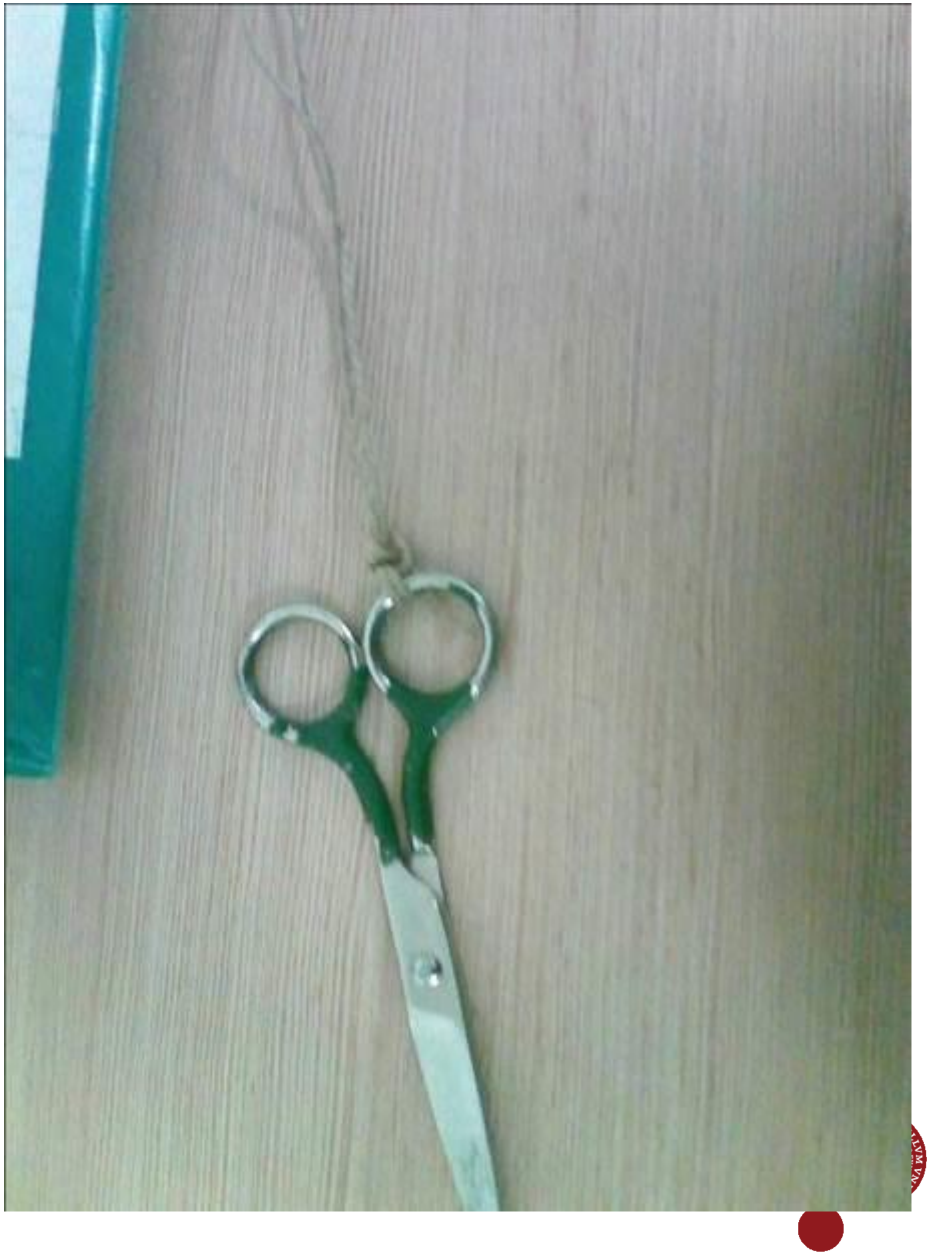
職　業　□学生　□会社員　□パート・アルバイト　□専業主婦　□フリーター
□その他（　　）

ダイレクトメール・Eメールなどでのご案内送付について
□ダイレクトメール可　□Eメール可

ご来店の動機
□紹介（　　様より）　□チラシを見て　□看板を見て
□その他（　　）

●ご要望などございましたら、ご記入ください。

顧客コード：　　担当者：



Handling risks

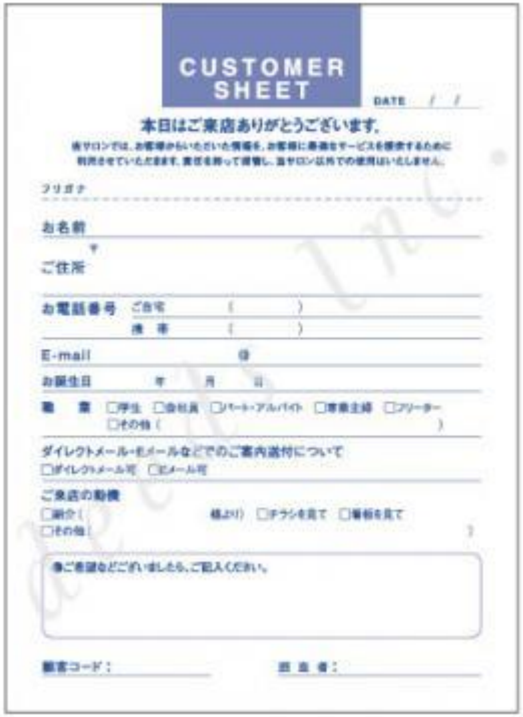
Eliminate/Mitigate

Minimize (compensate)

Transfer

Accept

~~Ignore~~



CUSTOMER SHEET

DATE / /

本日はご来店ありがとうございます。

当サロンでは、お客様からいただいた情報を、お客様に最適なサービスを提供するために利用させていただきます。責任を持って保管し、当サロン以外での使用はいたしません。

フリガナ

お名前

〒

ご住所

お電話番号 ご自宅 ( )

携帯 ( )

E-mail @

お誕生日 年 月 日

職業 □学生 □会社員 □パート・アルバイト □専業主婦 □フリーター

□その他 ( )

ダイレクトメール・Eメールなどでのご案内送付について

□ダイレクトメール可 □Eメール可

ご来店の動機

□紹介（ 様より） □チラシを見て □看板を見て

□その他（ ）

●ご要望などございましたら、ご記入ください。

顧客コード：

担当者：

Eliminate/Mitigate

Minimize (compensate)

Transfer

Accept

~~Ignore~~

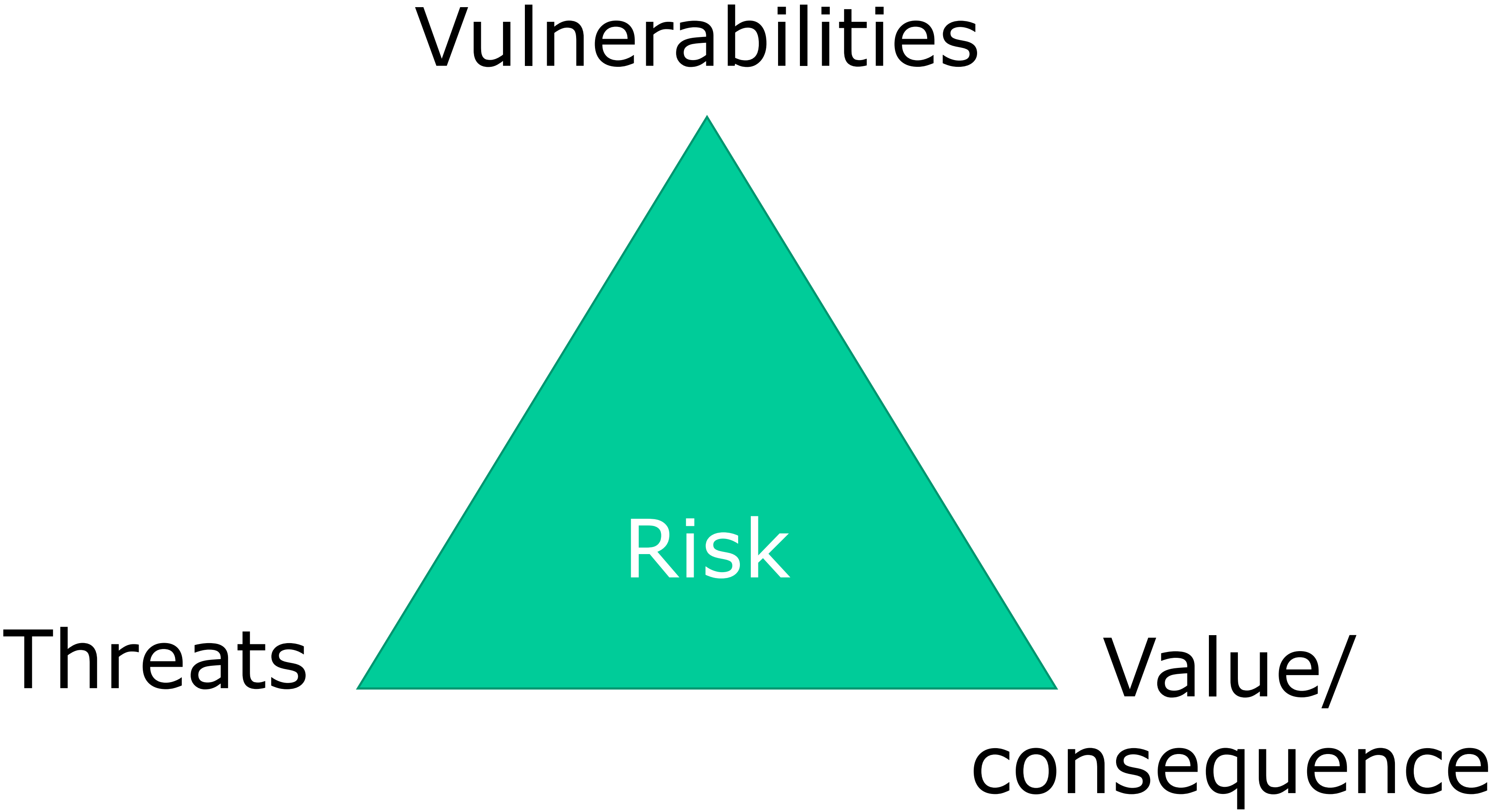
Risk assessment – definitions

Threat (trussel)
Vulnerability (sårbarhed)
Risk (risiko)
Exploit (exploit)
Asset (aktiv)

Eksempel 1 (Grækenland):
Risiko: Archilles død
Aktiv: Archilles liv
Sårbarhed: Archilles hæl
Trussel: Paris, skød Archilles i hælen med en pil
Exploit: Paris' pil

Richard Bejtlich - Taosecurity

Risk assessment



Vulnerabilities

Risk

Threats

Value/ consequence

Different approaches to risk assessment

How do you identify relevant risks and threats?

Threat assessment

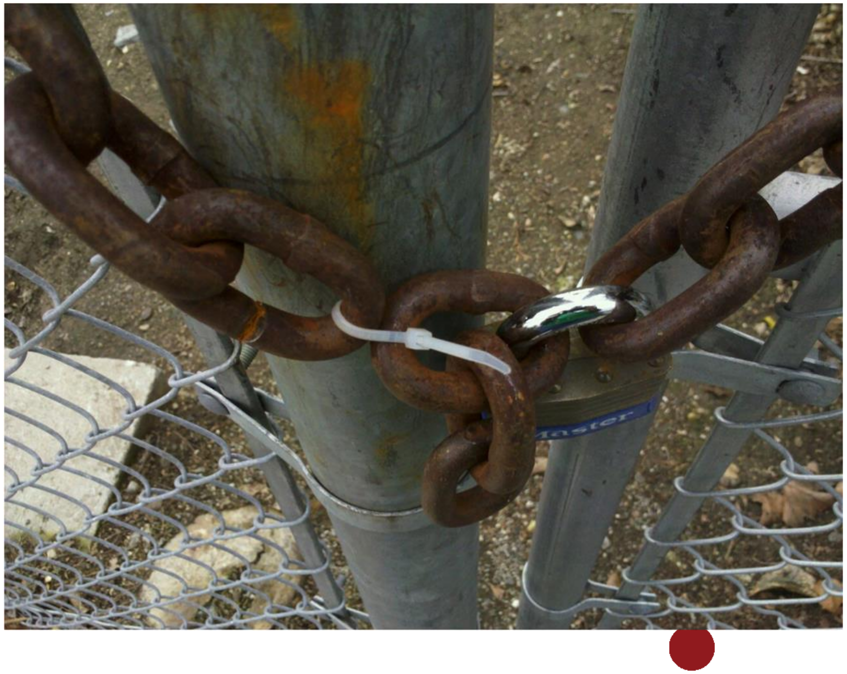
Risk modeling >< **Risk assessment**

Threats and risks

Threat assessments asks
"what could happen to this box/system/data?"

Risk assessments asks
"how much should I care?"

Playground in a kindergarden
or
Gate to a bank



Simple assessment

Would someone get angry if the information was left in a taxi?

How angry?

Security objectives: Clear objectives, determine how much effort to spend on subsequent steps.

Always know what you are assessing

Security objectives helps (a lot).
Always avoid broad statements such as

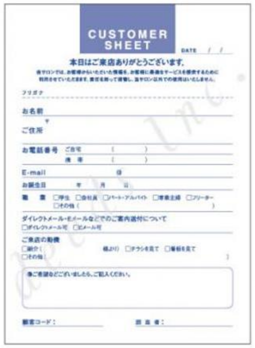
- ”Er det sikkert at bruge internettet?”
- ”Hvad er den bedste sikkerhedsløsning?”
- ”Er det sikkert at bruge cloud computing?”
- ”Må medarbejderne bruge Android-telefoner?”
- ”Afdeling Århus har lavet en iPad-løsning til sælgerne, de bruger Salesforce, er det ok?”

Different approaches to risk assessment

Threat assessment

Risk modeling >< Risk assessment

A security solution



CUSTOMER SHEET

DATE / /

本日はご来店ありがとうございます。

当サロンでは、お客様からいただいた情報を、お客様に最適なサービスを提供するために利用させていただきます。責任を持って管理し、当サロン以外での使用はいたしません。

フリガナ

お名前

〒

ご住所

お電話番号 ご自宅 （ ）
携 帯 （ ）

E-mail @

お誕生日 年 月 日

職 業 □学生 □会社員 □パート・アルバイト □専業主婦 □フリーター
□その他（ ）

ダイレクトメール・Eメールなどでのご案内送付について
□ダイレクトメール可 □Eメール可

ご来店の動機
□紹介（ 様より） □チラシを見て □看板を見て
□その他（ ）

※ご意見などございましたら、ご記入ください。

顧客コード： 担当者：

What are we protecting
What can go wrong
Who could do something

What is the consequence

Threat modeling – the 5 questions

1. What do you want to protect?
2. Who do you want to protect it from?
3. How likely is it that you will need to protect it?
4. How bad are the consequences if you fail?
5. How much trouble are you willing to go through in order to try to prevent those?

Threat modeling – the 5 questions

1. What do you want to protect?
   Assets
2. Who do you want to protect it from?
   Adversaries and threats
3. How likely is it that you will need to protect it?
   Probability
4. How bad are the consequences if you fail?
   Risk
5. How much trouble are you willing to go through in order to try to prevent those?
   Value

Threat modeling

Do threat modeling early in the process – otherwise security becomes a bug-hunting exercise (not effective)

Purpose of threat modeling is primarily to find security DESIGN errors

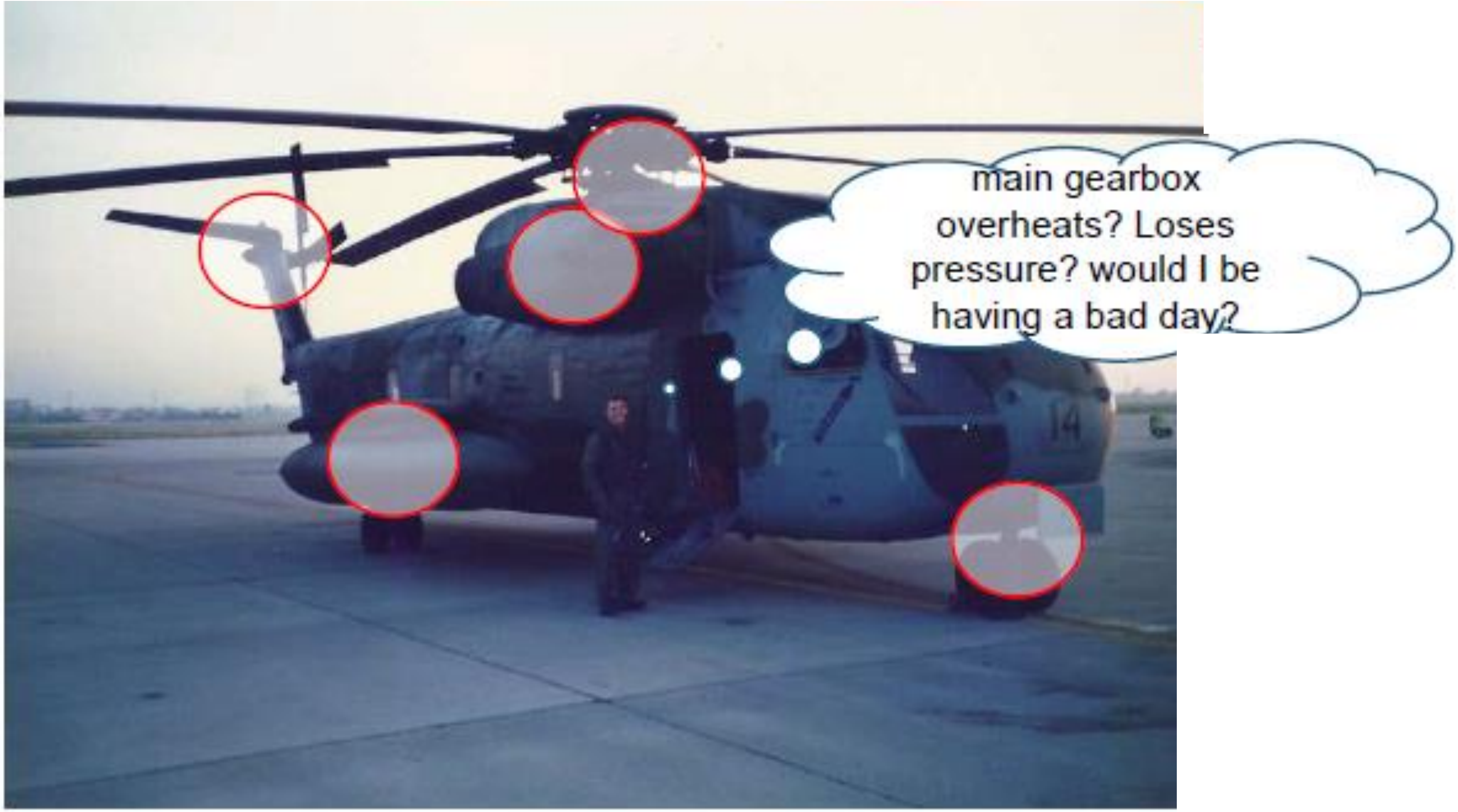
Know your assets first

Need to know what you are protecting

- Data and information: Data for running your business, design documents, data about customers, data about your identity, software
- Reputation, brand name
- Responsiveness
- Personal safety
- Physical assets: servers, laptops, mobile phones, …

Assets should have an associated value (e.g., cost to replace, cost to reputation, importance to business operation)

Step 1: Mapping processes and assets

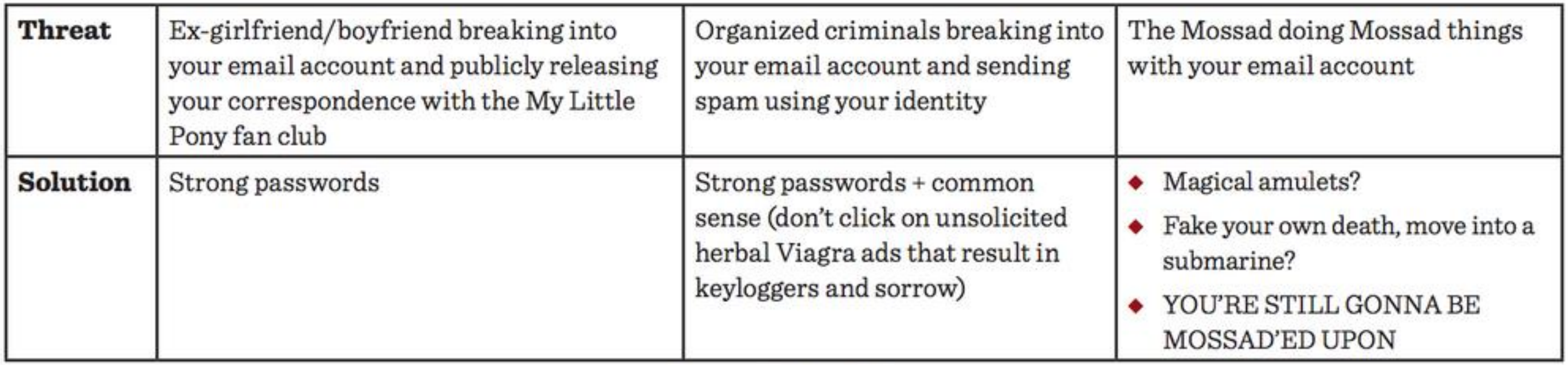


main gearbox overheats? Loses pressure? would I be having a bad day?

Adversaries

Hacktivists
Organised crime
Terrorists
National governments
Thieves
Business competitors
Industrial espionage
Your supplier
Your consumer
The media
Your family
Your ex-girlfriend
…

Threat models

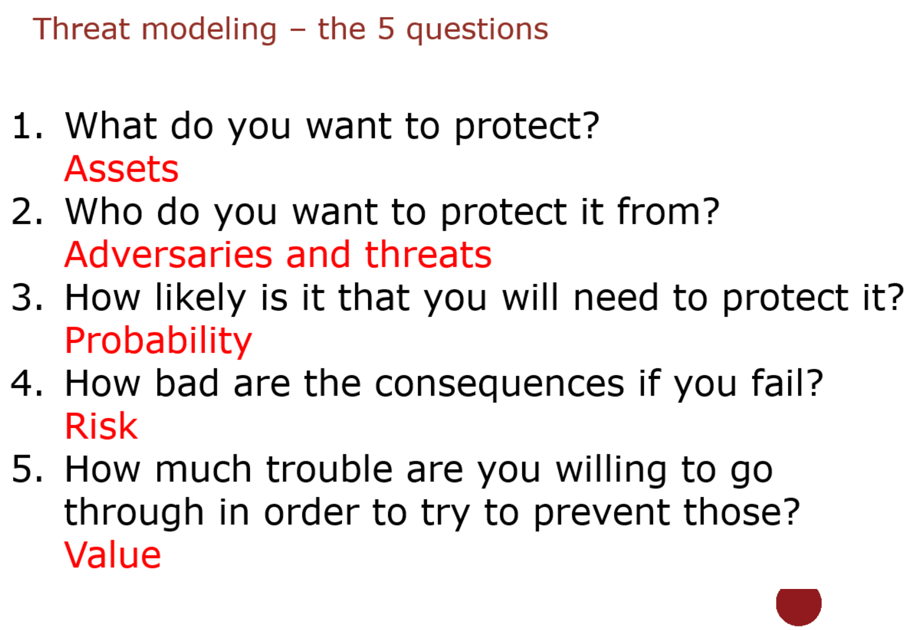


Threat	Ex-girlfriend/boyfriend breaking into your email account and publicly releasing your correspondence with the My Little Pony fan club	Organized criminals breaking into your email account and sending spam using your identity	The Mossad doing Mossad things with your email account
Solution	Strong passwords	Strong passwords + common sense (don't click on unsolicited herbal Viagra ads that result in keyloggers and sorrow)	◆ Magical amulets? ◆ Fake your own death, move into a submarine? ◆ YOU'RE STILL GONNA BE MOSSAD'ED UPON

Figure 1: Threat models

Threat modeling – your life

Should I buy a new bicycle lock?
Should I lock the door at home?
Should I use Gmail?



Threat modeling – the 5 questions

1. What do you want to protect?
   Assets
2. Who do you want to protect it from?
   Adversaries and threats
3. How likely is it that you will need to protect it?
   Probability
4. How bad are the consequences if you fail?
   Risk
5. How much trouble are you willing to go through in order to try to prevent those?
   Value

Threat modeling – important

Distinguish between threats and risks

A threat is a bad thing that can happen
Risk is the likelihood that the threat will occur

There is a threat that your building might collapse, but the risk of this happening is far greater in California than in Denmark

Don’t lose the distinction between
”what’s possible” and ”what’s probable”

Risikovurdering – oversvømmelse af serverrum

Trussel: Oversvømmelse

Sårbarhed: Serverrummet er i kælderen

Sandsynlighed: Erfaringen er, at vi får en oversvømmelse hver 20. år. Med de nuværende klimaforandringer forventer vi, at der vil komme oversvømmelser fra havnen hver 5. år

Konsekvens: Kælder oversvømmes og vand ødelægger derved servere

Sikkerhedstiltag: Flytning af serverrum til 3.sal kan fjerne sårbarhed, alternativt outsource/cloudsource

Different approaches

Many ways to go about security analyses, including:

- Asset-centric
- Vulnerability-centric
- Threat-centric

See also OWASP Threat Risk Modeling

How to actually do threat modeling?

Must be a repeatable process to find and address all relevant threats

Brainstorm based on experience (requires a lot of experience to do well)

Other methods such as risk catalogues – or you can use models

Data flow mapping and risk analysis models

A repeatable process to document required data and to find and address relevant threats

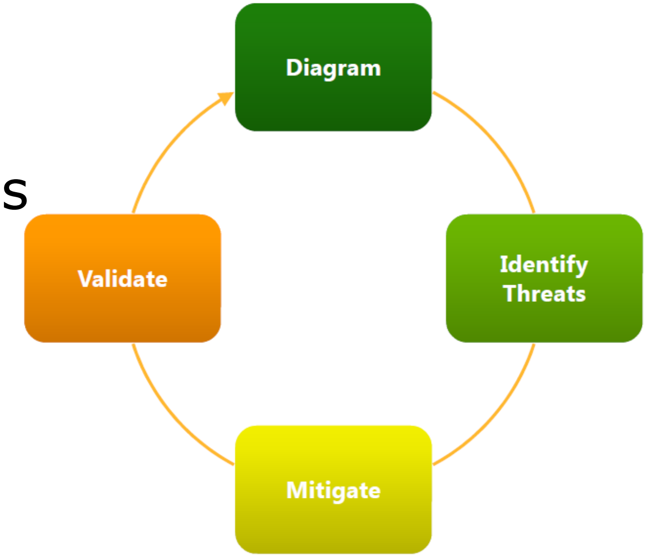
Find problems when there's time to fix them. The earlier you start, the more time to plan and to fix.

Threat model

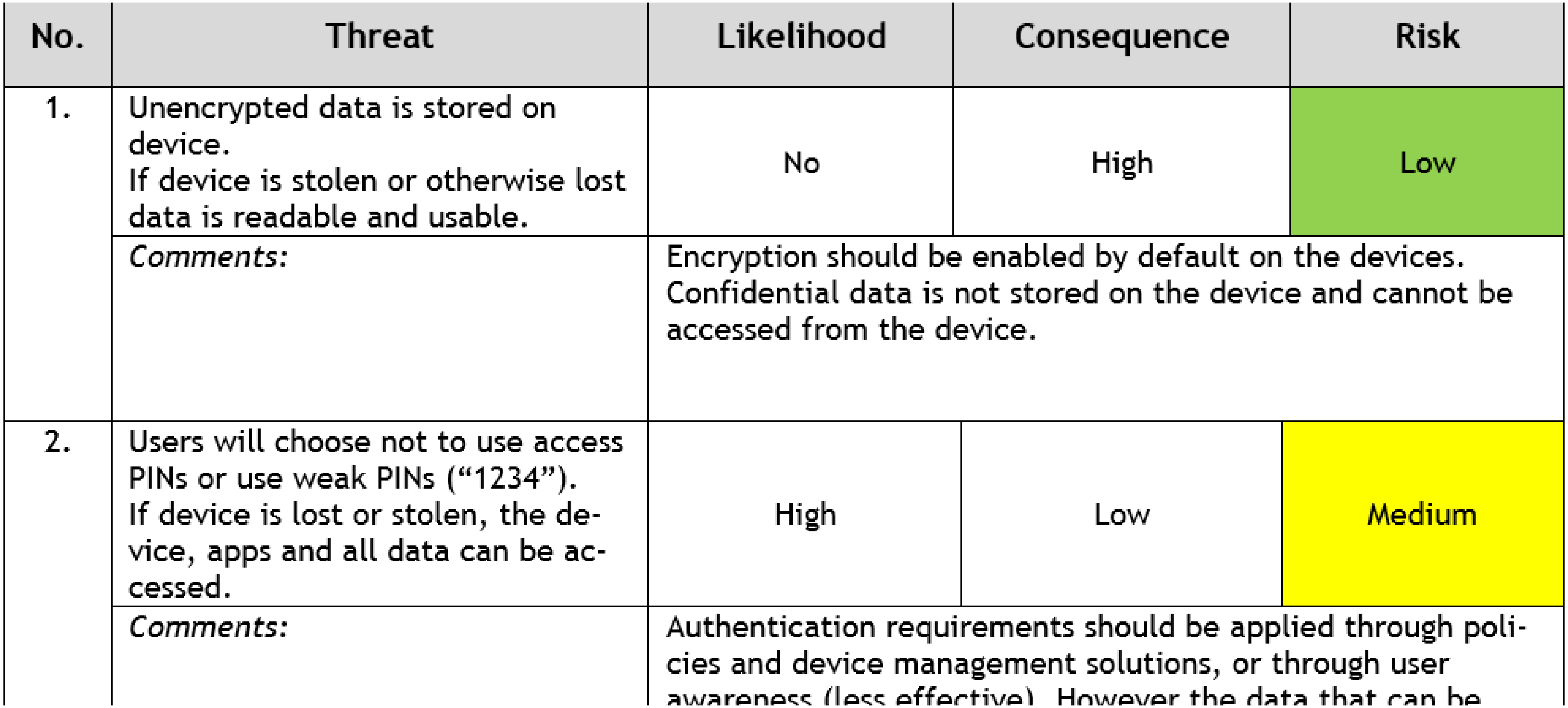
– Look at the product/process as a whole

– identify it-security/privacy relevant features

- Identify attack surfaces



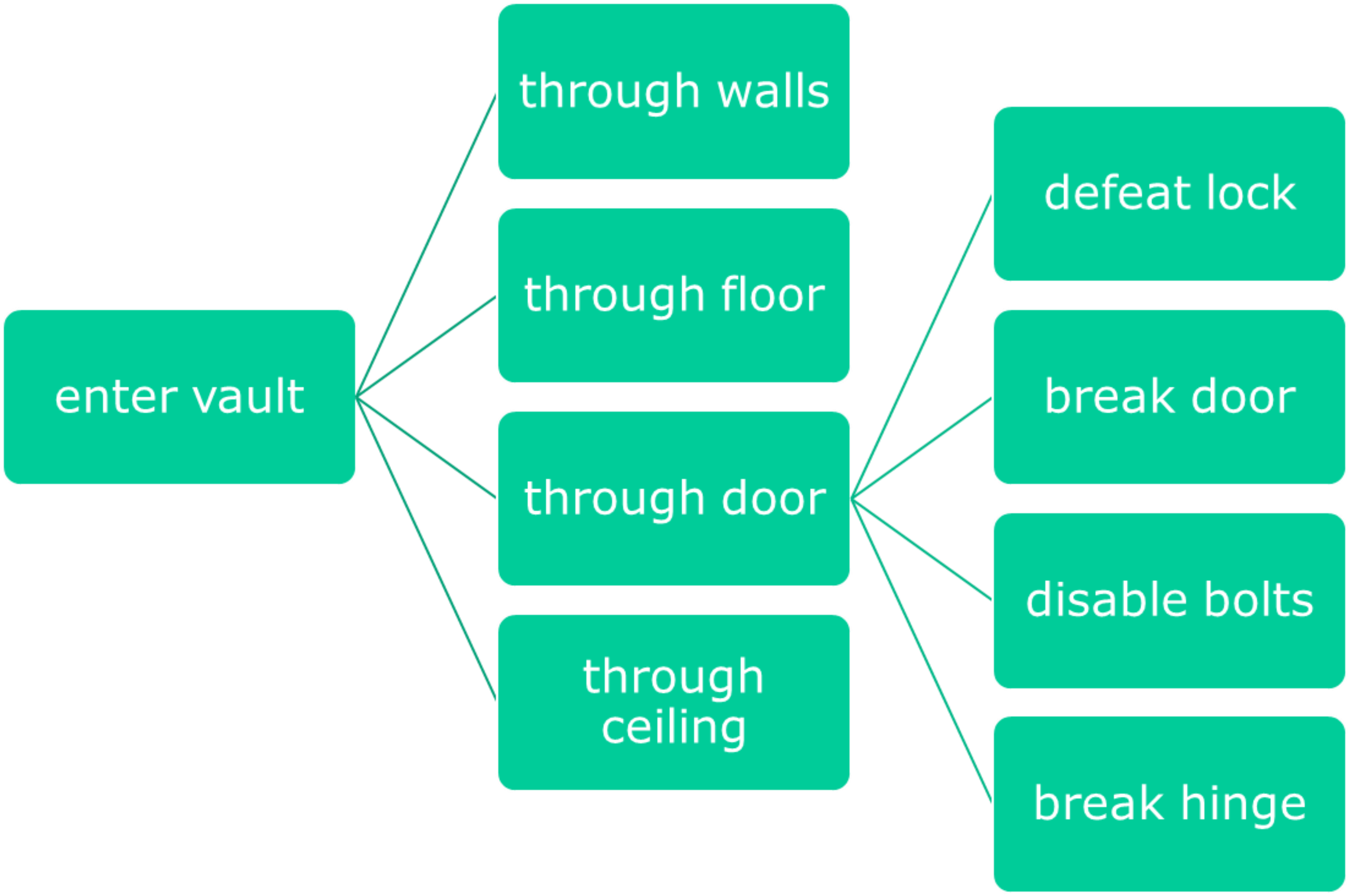
Risk assessment - application



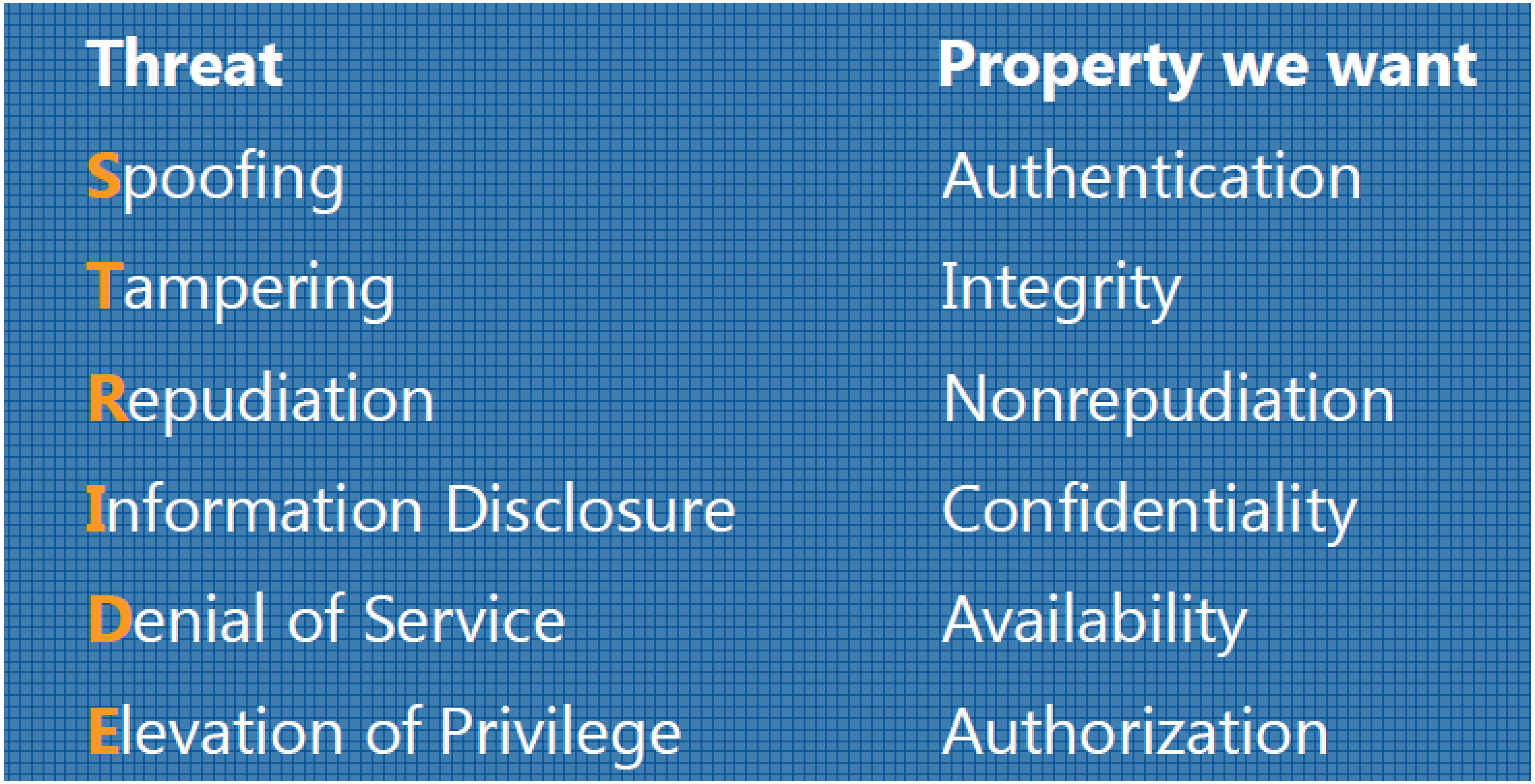
No.	Threat	Likelihood	Consequence	Risk
1.	Unencrypted data is stored on device. If device is stolen or otherwise lost data is readable and usable.	No	High	Low
	Comments:	Encryption should be enabled by default on the devices. Confidential data is not stored on the device and cannot be accessed from the device.		
2.	Users will choose not to use access PINs or use weak PINs ("1234"). If device is lost or stolen, the device, apps and all data can be accessed.	High	Low	Medium
	Comments:	Authentication requirements should be applied through policies and device management solutions, or through user awareness (less effective). However the data that can be		

More in the Security Management lecture

Threat / attack trees

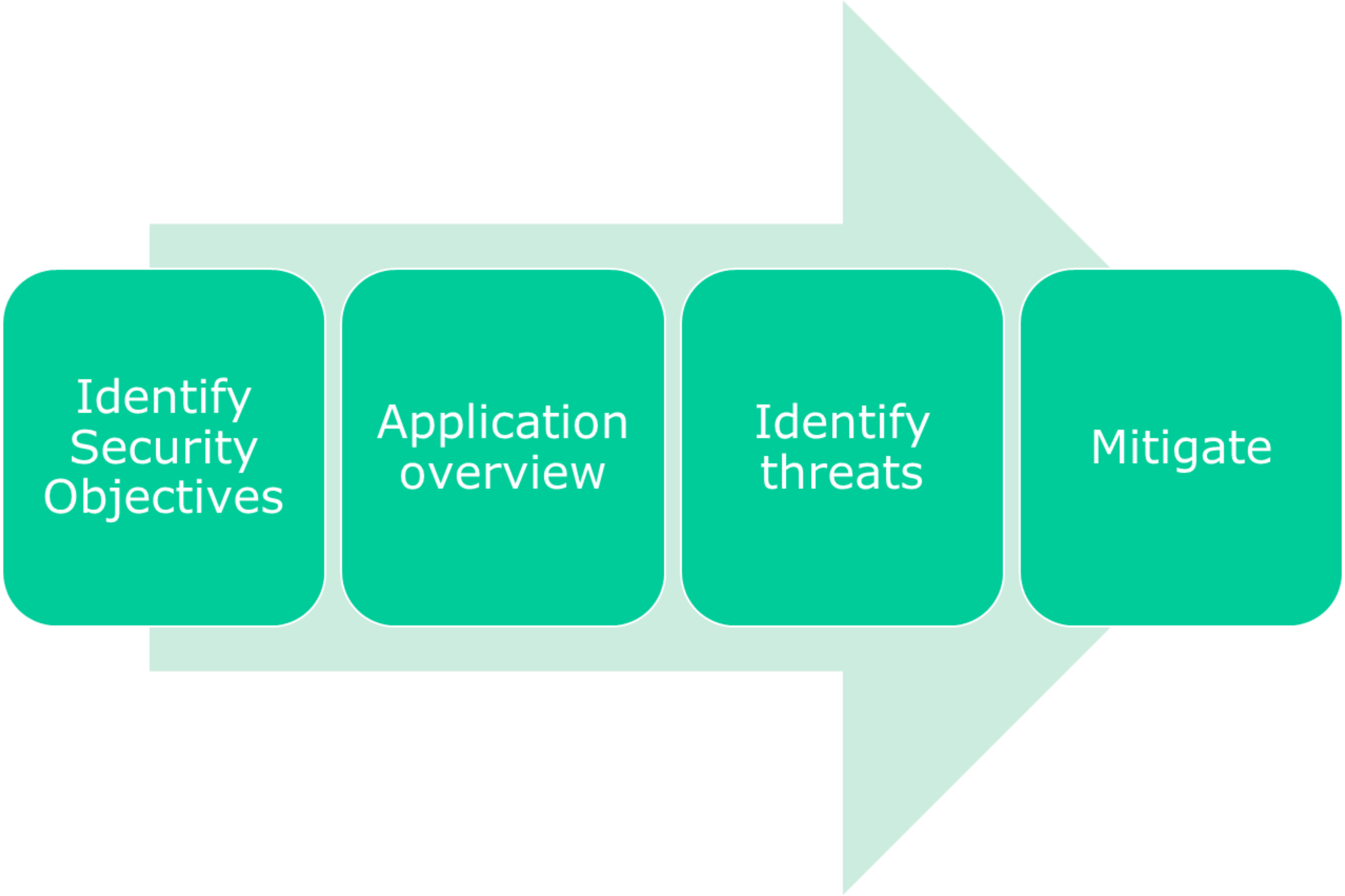


The STRIDE model

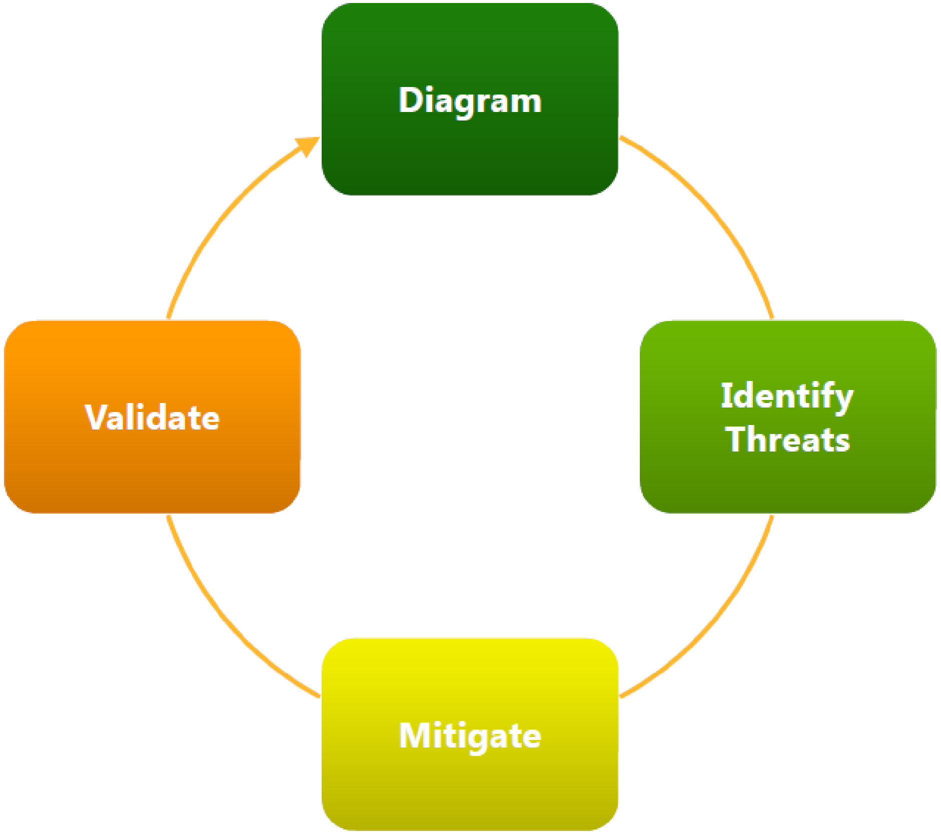


Threat	Property we want
Spoofing	Authentication
Tampering	Integrity
Repudiation	Nonrepudiation
Information Disclosure	Confidentiality
Denial of Service	Availability
Elevation of Privilege	Authorization

STRIDE


Identify Security Objectives
Application overview
Identify threats
Mitigate

Stride: Data flow mapping



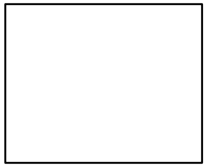
Diagram

Identify Threats

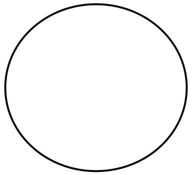
Mitigate

Validate

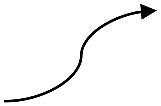
Tool – STRIDE diagram elements



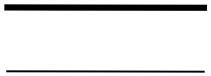
People, systems
entities



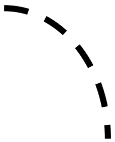
Process, service
components



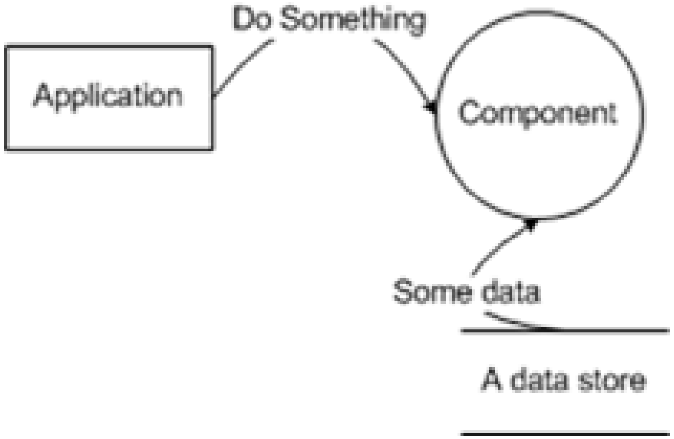
Dataflow,
traffic, system calls



Data store, database,
file, queue



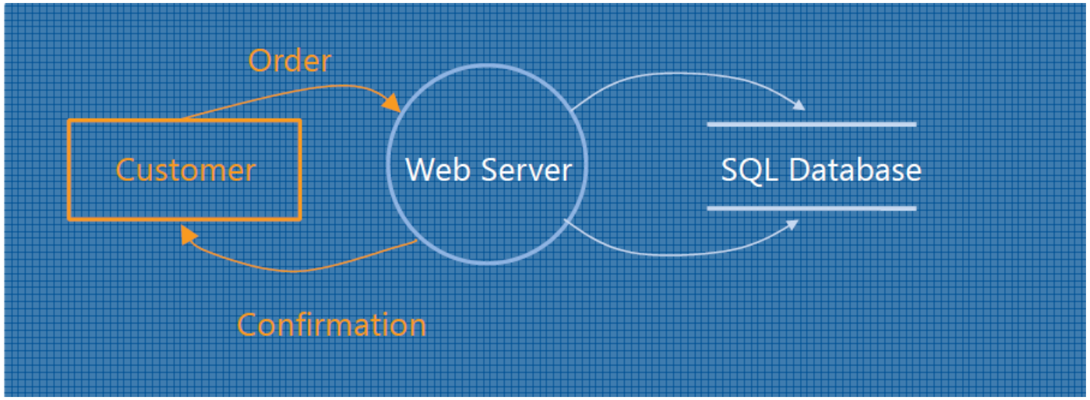
Trust boundary,
file system, process
boundary, company



STRIDE data flow drawings can be made in several layers

Context Diagram

Very high-level drawing; the entire business / system / component / product



Data flow mapping – diagram layers

- Context Diagram

– Very high-level; entire component / product / system

- Level 1 Diagram

– High level; single feature / scenario

- Level 2 Diagram

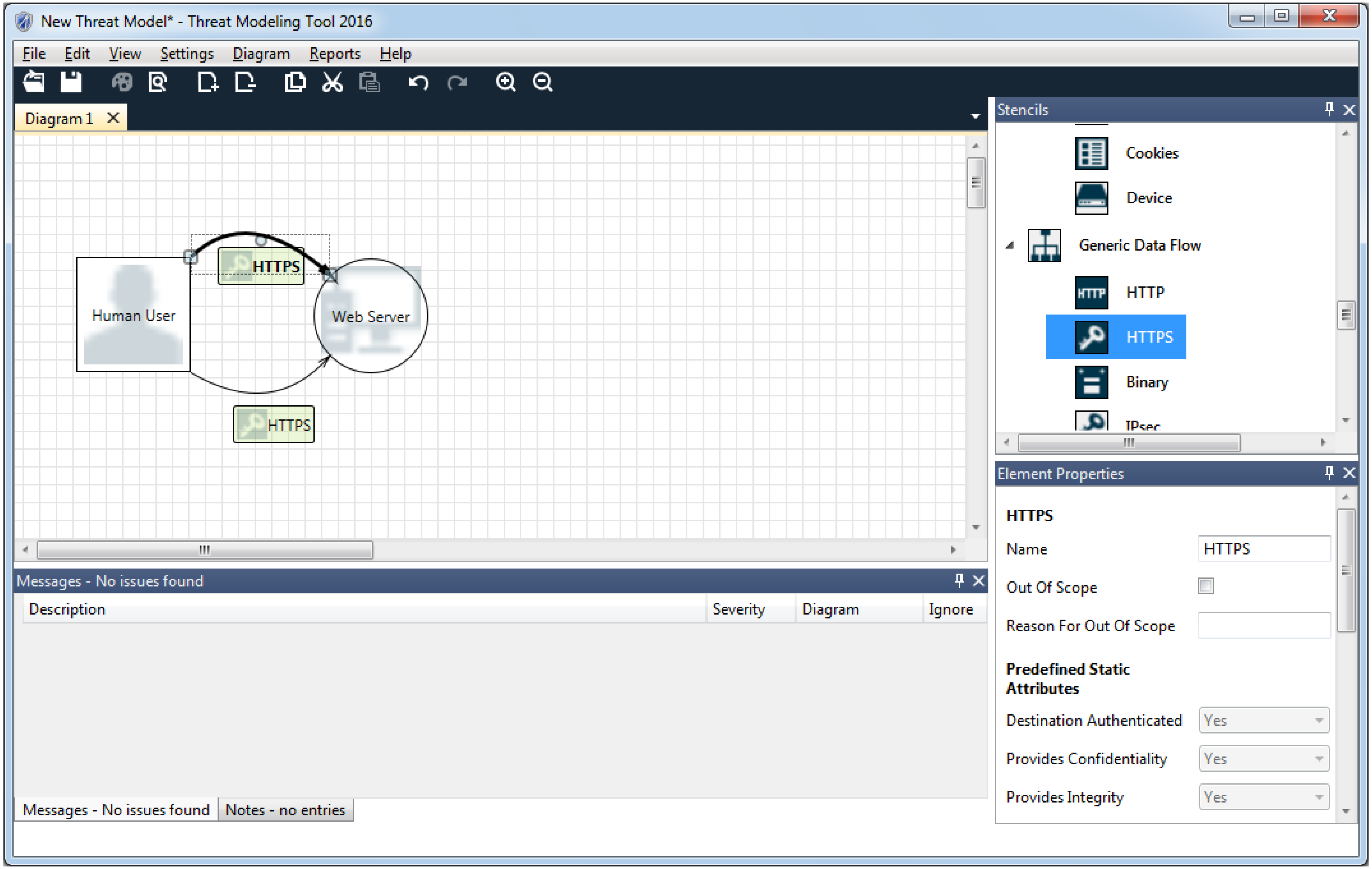
– Low level; detailed sub-components of features

- Level 3 Diagram

– More detailed

– Rare to need more layers, except in huge projects or when you're drawing more trust boundaries

Context level flow



New Threat Model* - Threat Modeling Tool 2016

Diagram 1

Human User

HTTPS

Web Server

HTTPS

Messages - No issues found

Description	Severity	Diagram	Ignore

Messages - No issues found | Notes - no entries

Stencils: Cookies, Device, Generic Data Flow, HTTP, HTTPS, Binary, IPsec

Element Properties

HTTPS

Name: HTTPS

Out Of Scope: □

Reason For Out Of Scope:

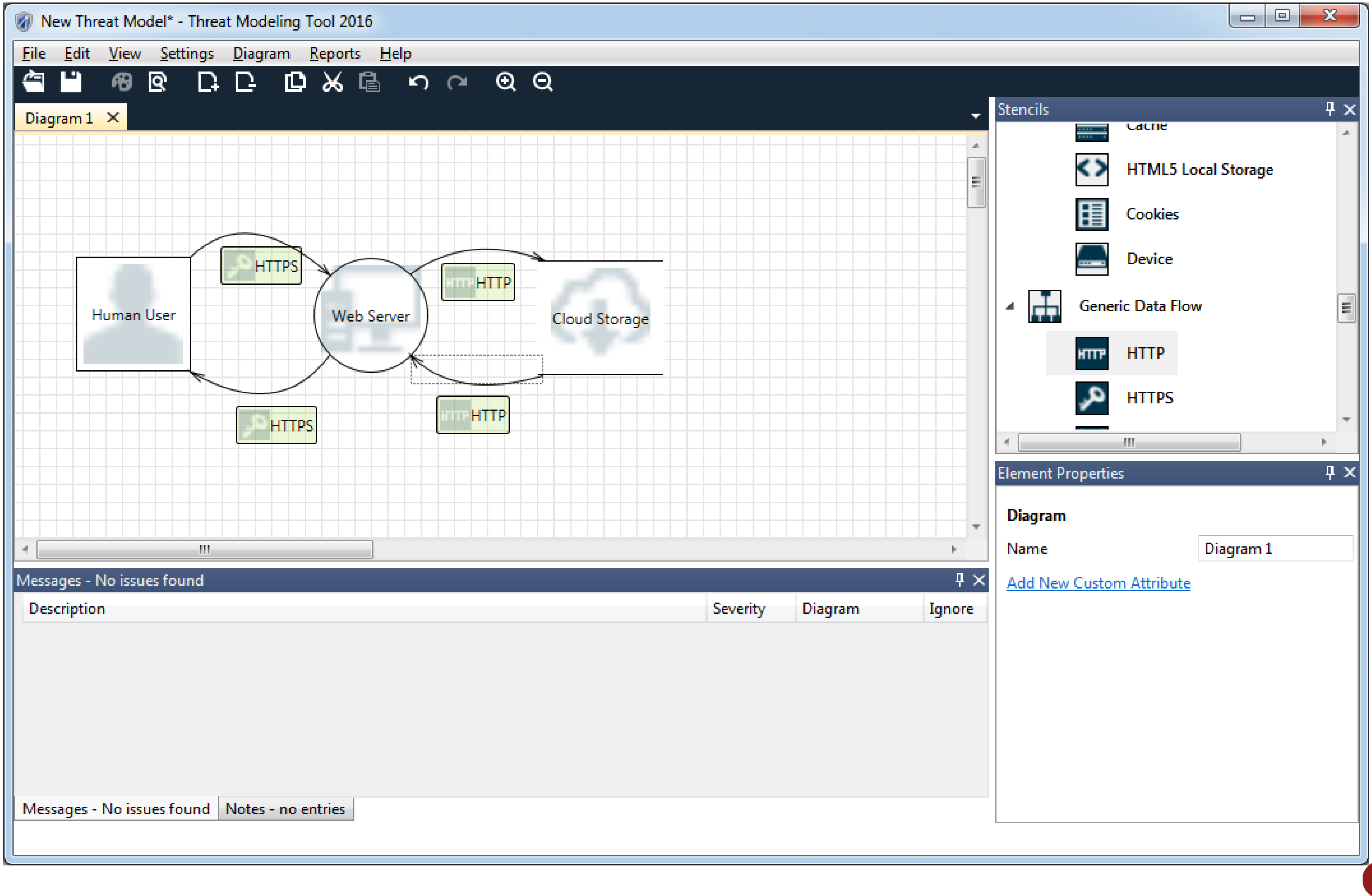
Predefined Static Attributes

Destination Authenticated: Yes

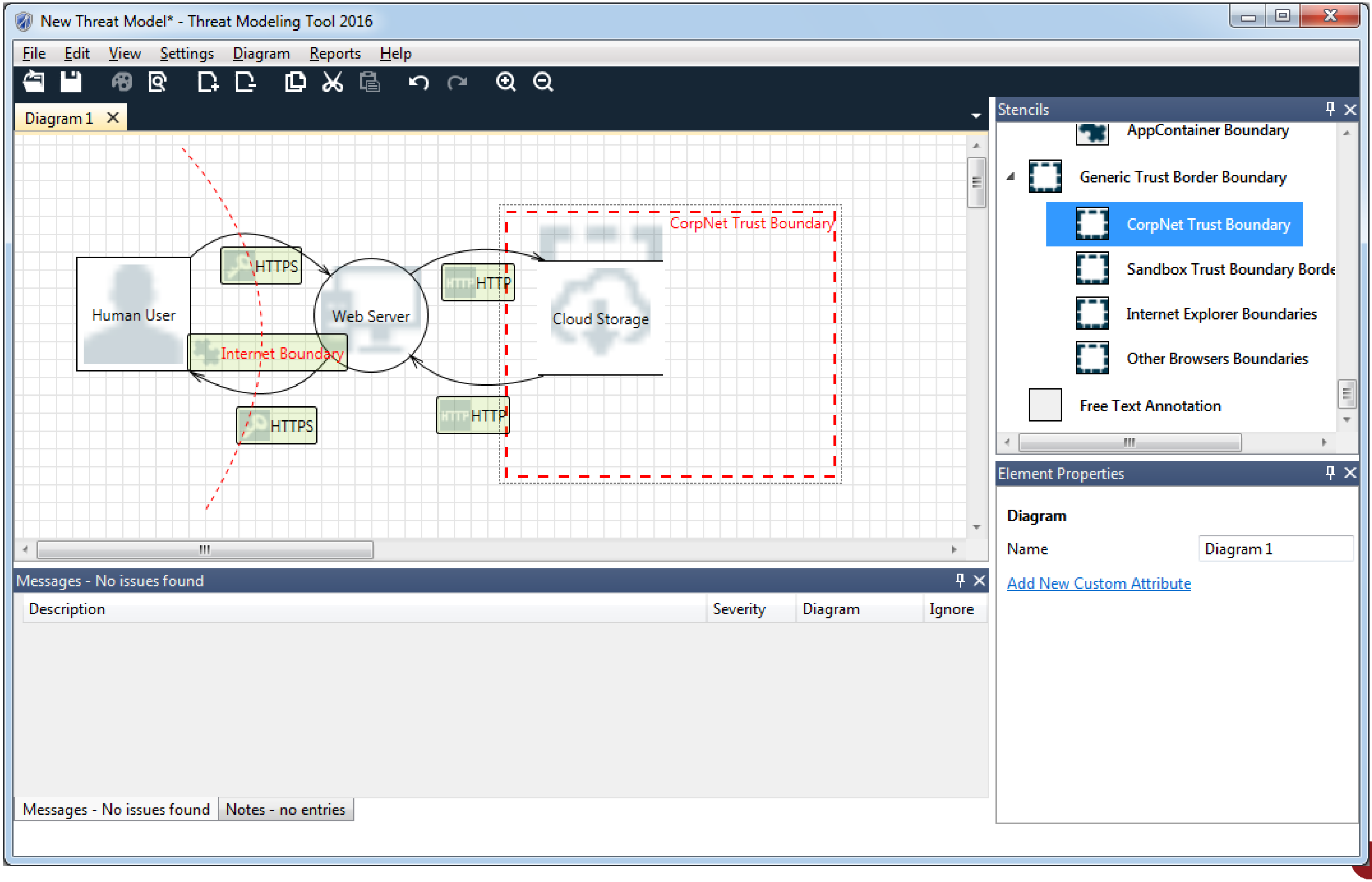
Provides Confidentiality: Yes

Provides Integrity: Yes

Context level flow



Context level flow



New Threat Model* - Threat Modeling Tool 2016

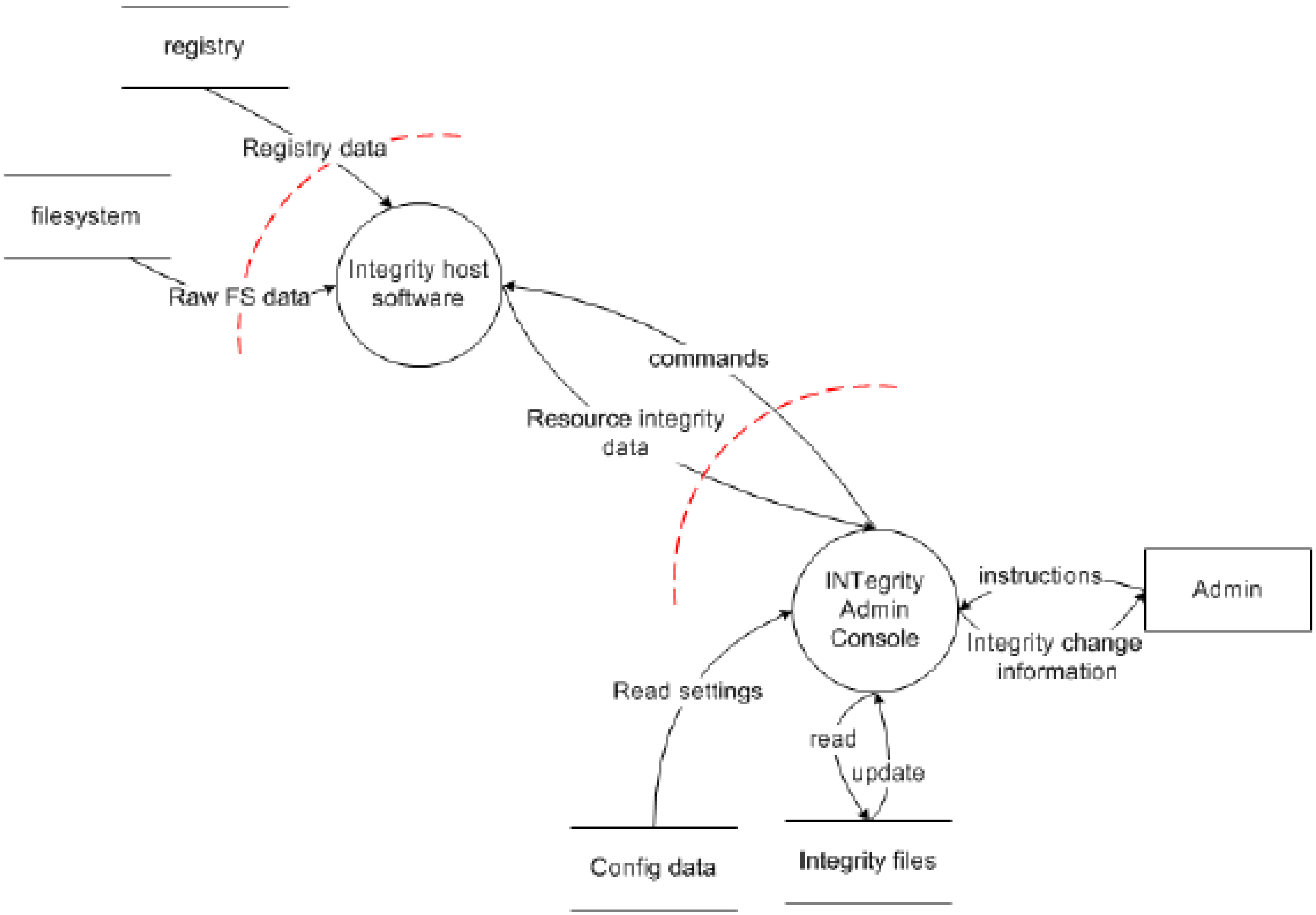
Messages - No issues found

Description	Severity	Diagram	Ignore

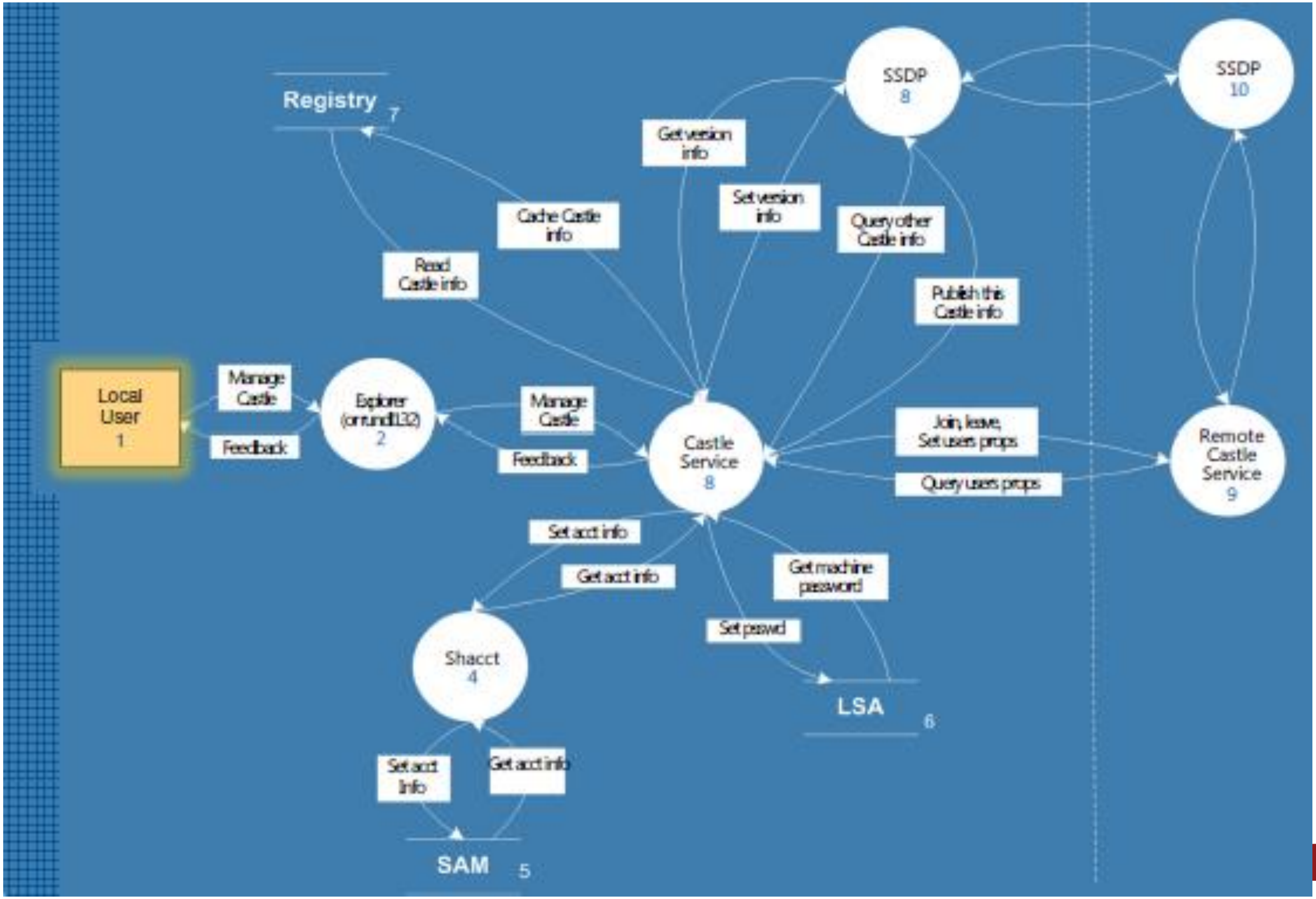
Diagram

Name: Diagram 1

Data flow mapping - drawing

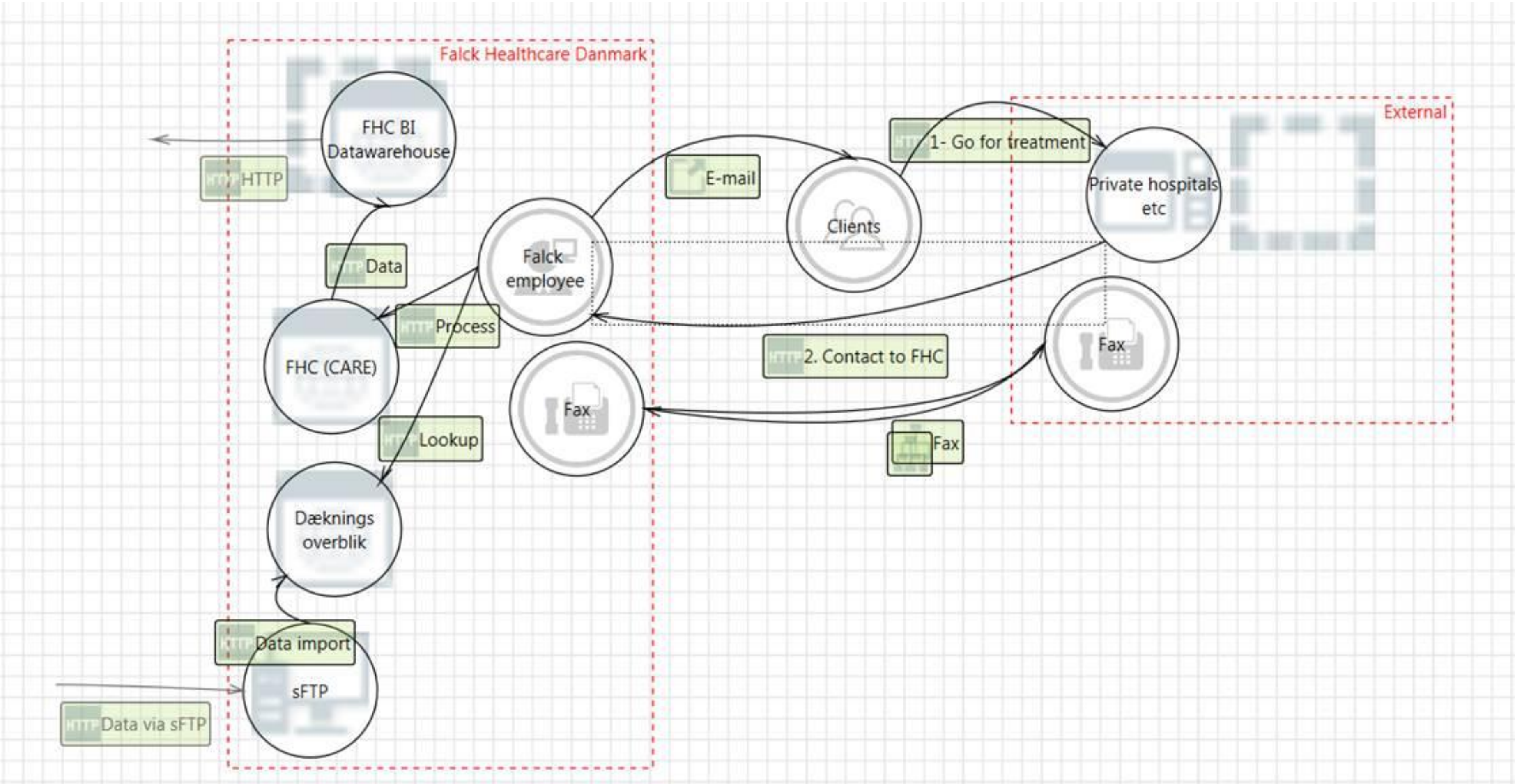


Data flow mapping - drawing

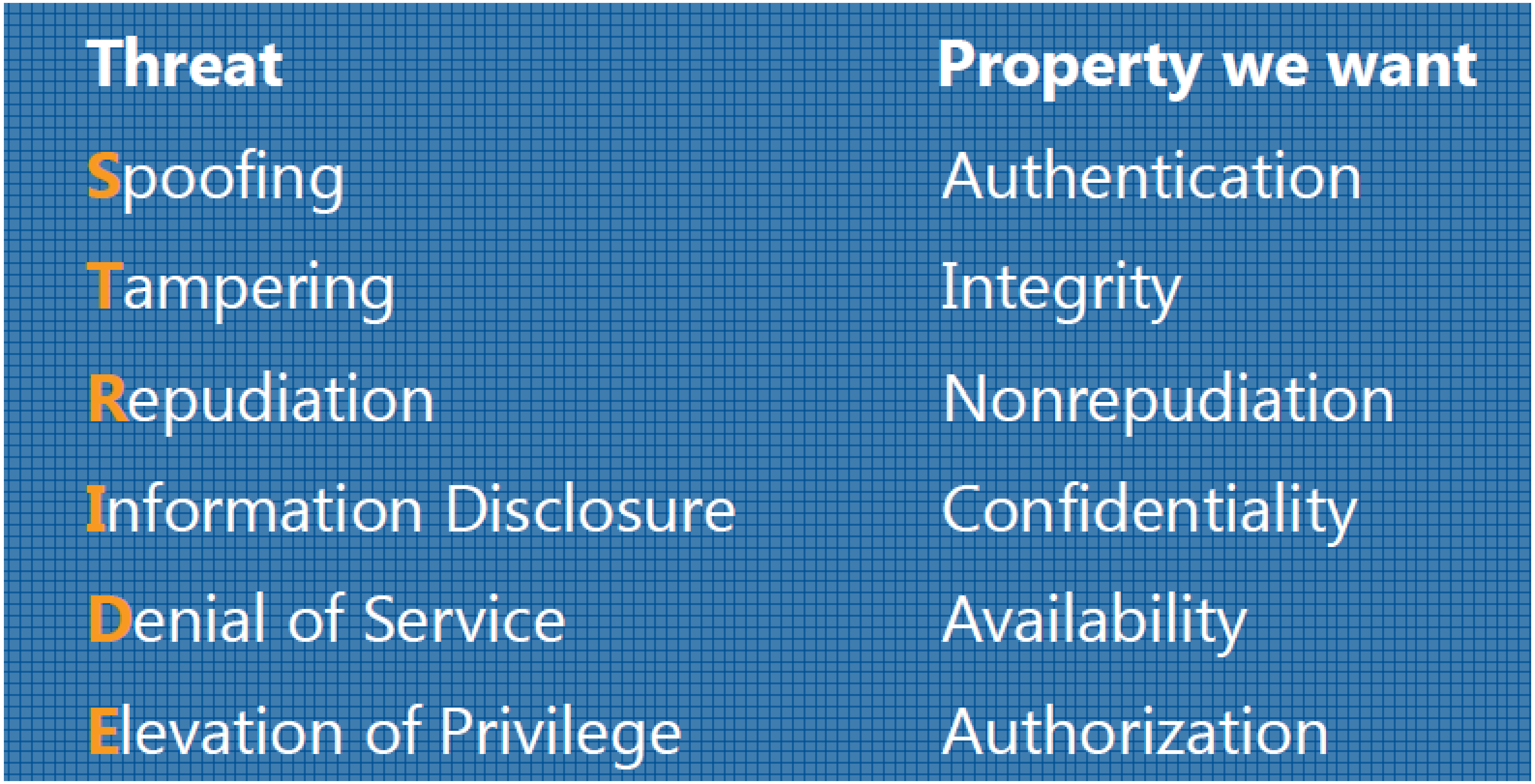


Sample ”Level 1” process flow

Customer process

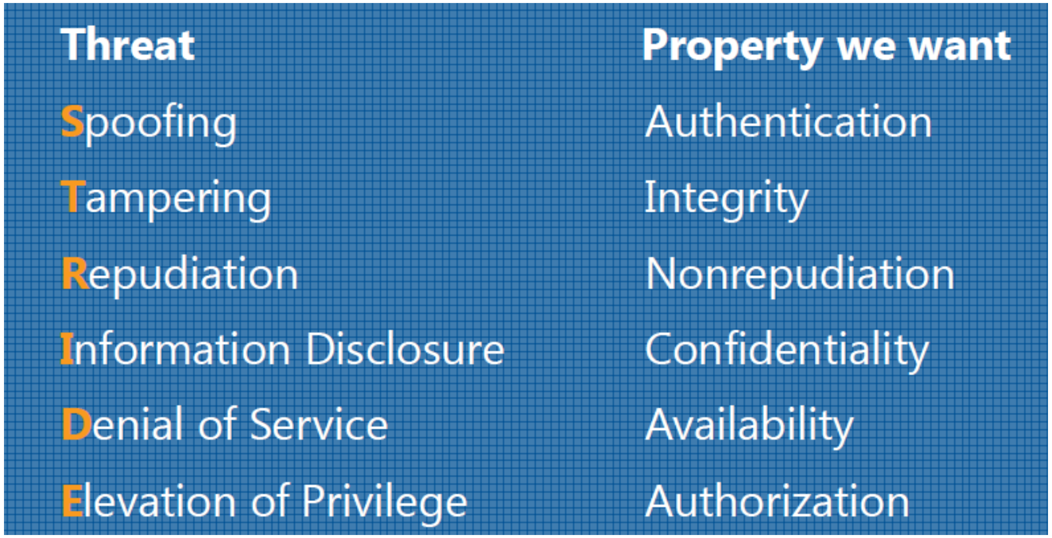


The STRIDE model – Step 2 Threat assessment



Threat	Property we want
Spoofing	Authentication
Tampering	Integrity
Repudiation	Nonrepudiation
Information Disclosure	Confidentiality
Denial of Service	Availability
Elevation of Privilege	Authorization

Stride



Threat	Property we want
Spoofing	Authentication
Tampering	Integrity
Repudiation	Nonrepudiation
Information Disclosure	Confidentiality
Denial of Service	Availability
Elevation of Privilege	Authorization

Spoofing - Impersonating something or someone else

Tampering - Modifying data or code

Repudiation - Claiming to have not performed an action

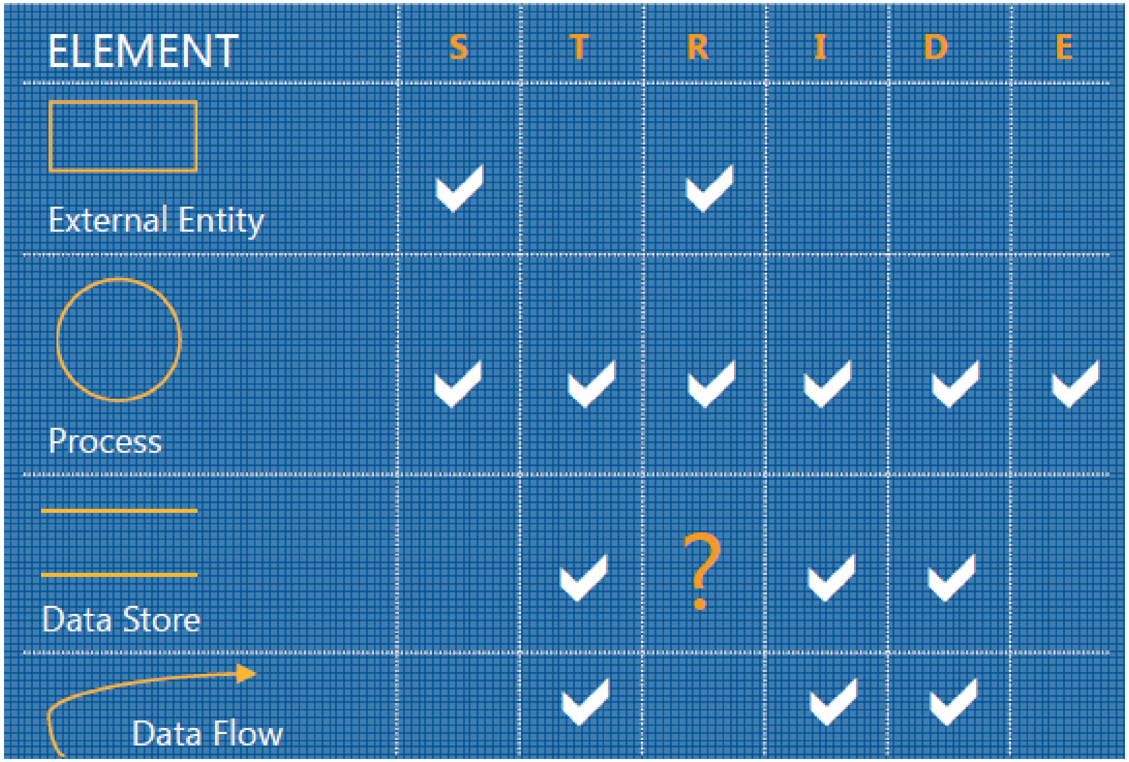
Info Disclosure - Exposing information to someone not authorized to see it

Denial of Service - Deny or degrade service to users

Elevation of Privilege - Gain capabilities without proper authorization

Threats, not **vulnerabilities !**

Use STRIDE on the diagram elements

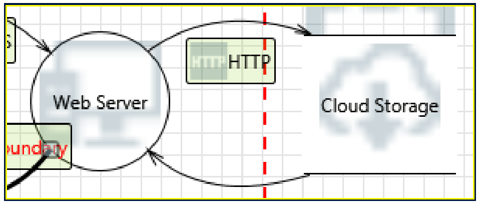


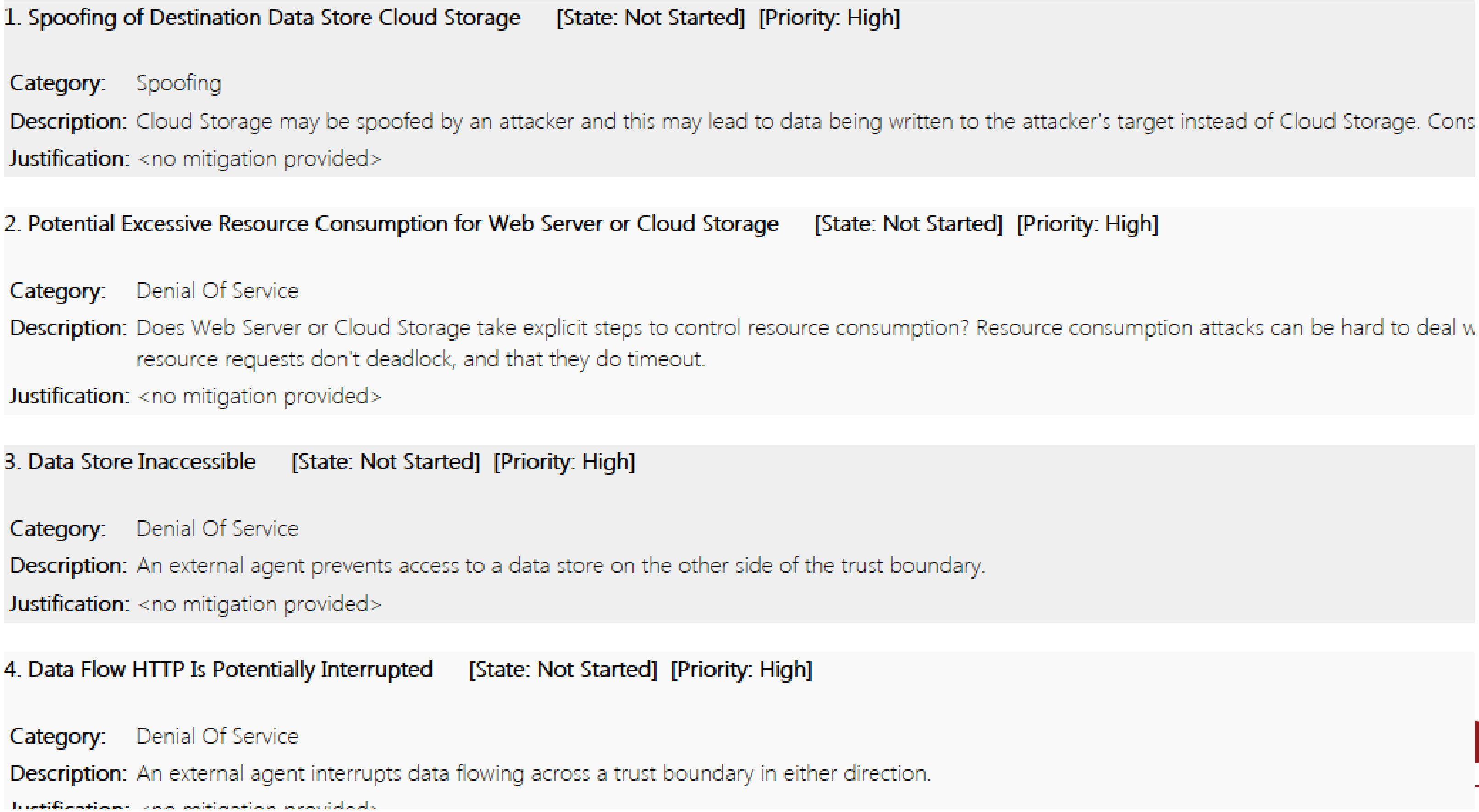
ELEMENT	S	T	R	I	D	E
External Entity	✓		✓			
Process	✓	✓	✓	✓	✓	✓
Data Store		✓	?	✓	✓	
Data Flow		✓		✓	✓	

Spoofing
Tampering
Repudiate
Info disclosure
Denial of Service
Elevate privilege

Tool – Context level flow

Interaction: HTTP





1. Spoofing of Destination Data Store Cloud Storage [State: Not Started] [Priority: High]

Category: Spoofing
Description: Cloud Storage may be spoofed by an attacker and this may lead to data being written to the attacker's target instead of Cloud Storage. Cons
Justification: <no mitigation provided>

2. Potential Excessive Resource Consumption for Web Server or Cloud Storage [State: Not Started] [Priority: High]

Category: Denial Of Service
Description: Does Web Server or Cloud Storage take explicit steps to control resource consumption? Resource consumption attacks can be hard to deal w resource requests don't deadlock, and that they do timeout.
Justification: <no mitigation provided>

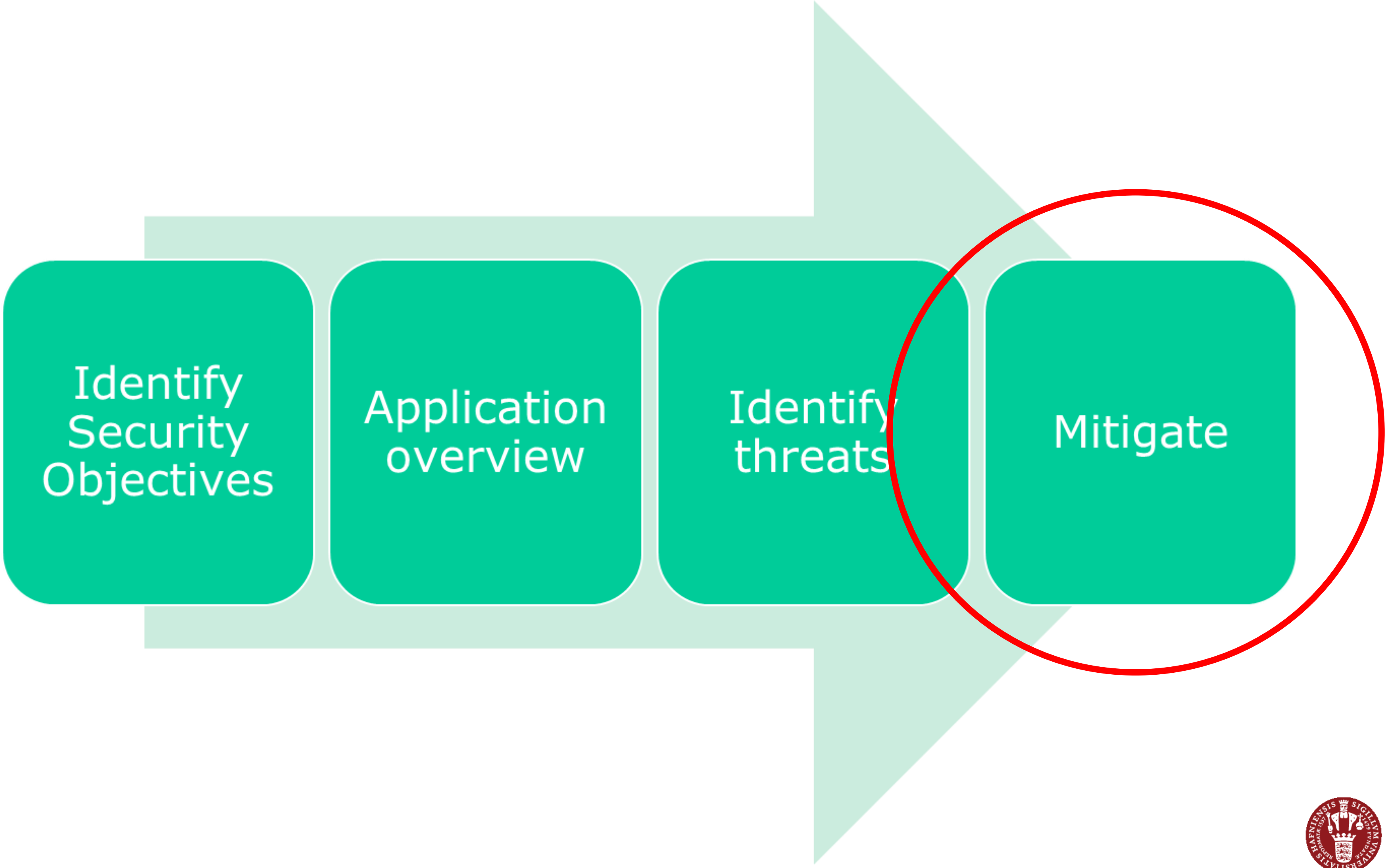
3. Data Store Inaccessible [State: Not Started] [Priority: High]

Category: Denial Of Service
Description: An external agent prevents access to a data store on the other side of the trust boundary.
Justification: <no mitigation provided>

4. Data Flow HTTP Is Potentially Interrupted [State: Not Started] [Priority: High]

Category: Denial Of Service
Description: An external agent interrupts data flowing across a trust boundary in either direction.
Justification: <no mitigation provided>

STRIDE



Identify Security Objectives

Application overview

Identify threats

Mitigate

Countermeaures

IT security requirements should be identified and handled by a methodical assessment of the risks.

Are the risks tolerable?
Should we try to mitigate them, how?

This is where your security engineering toolbox comes into play

The whole system is critical

Secuity is only as strong as the weakest link

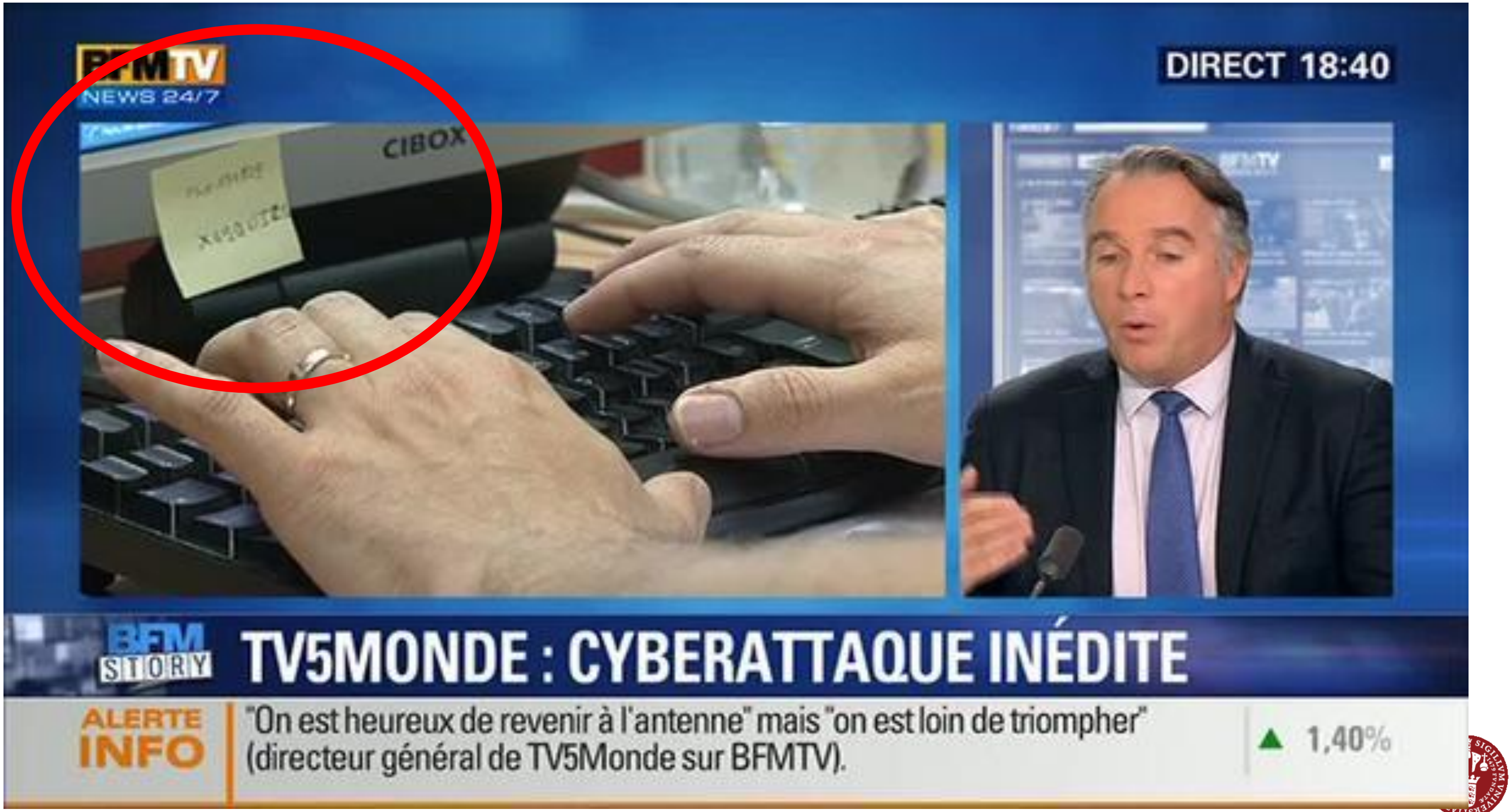
Securing a system involves a whole-system view:

- Cryptography
- Implementation
- People
- The computer environment (network of networks)
- Everything in between

"If you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology" – Bruce Schneier

You need to consider **people**, **processes**, **technology**

IT-security is fun (but not easy)



TV5MONDE : CYBERATTAQUE INÉDITE

"On est heureux de revenir à l'antenne" mais "on est loin de triompher" (directeur général de TV5Monde sur BFMTV).

?