



# Informatics and Sustainability

Internet and Reality – The real and the fake in the digital age  
HS2015 / Prof. Dr. M. Hilty

Hernani Marques Madeira <h2m@access.uzh.ch>

Matthias Scherrer <matthias.scherrer@uzh.ch>

Florian Schüpfer <flo.schuepfer@bluewin.ch>



**Universität  
Zürich** UZH

**Institut für Informatik**

# Digital Image Doctoring

## Digital Image Doctoring



## Cloning

- Technique
  - copy and pasting of objects
- Artifacts
  - repeating patterns in image
- Detection
  - find similar and spacially coherent image regions



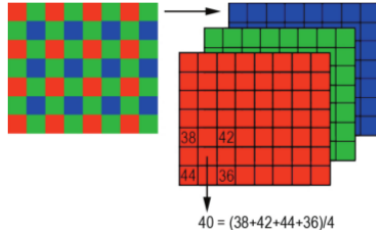
## Lighting

- Technique
  - move objects from one setting to another
- Artifacts
  - inconsistent light direction
- Detection
  - estimate direction of light by brightness distribution on surfaces
  - detect inconsistencies



## Re-touching

- Technique
  - adjusting colors / contrast / white balance, sharpness, noise, removing elements or visible flaws on skin or materials
- Artifacts
  - distorted correlations in color-sensor array
- Detection
  - detect wrong correlations



## Negative Effects

Propaganda  
(for / against  
persons or  
topics)



## Negative Effects

Alteration of history  
(removing objects or  
persons from  
historical images)







**Universität  
Zürich** <sup>UZH</sup>

**Institut für Informatik**

# YouTube views – fake or real?



## Advertisement on YouTube

- Enable AdSense on the account (account monetization)
- 45/55 split of all YouTube advertising
  - 45% for Google
  - 55% for the content creator
- Average cost per thousand YouTube views (2013): \$ 7.80





## Winners and Losers of fake views

- Advertisers are charged on the basis of how many times their advertisements are viewed.
- Winners:
  - (Google that charges for the advertisement)
  - Content creators who get a part of these revenues and probably more popularity than they would without boosting their view count.
- Losers:
  - Advertisers who pay for fake views → click fraud or “invalid traffic” as Google prefers to call it



## How to fake YouTube views?

- Low-wage work force
- Purchase fake YouTube views
- Purchase or program a bot/algorithm to increase the traffic figures:
  - \$ 250 billion spent by advertisers for marketing each year from which they probably lose \$ 6 billion to such bots/algorithms

## Not only YouTube views ...

- ... can be bought, also comments, likes, etc.
- A lot of other services can be bought as well.



The screenshot shows the homepage of YTview.com, a website for purchasing social media services. On the left, a blue banner reads "100% Satisfaction Guaranteed" with a blue arrow pointing to a cartoon character of a man in a suit and sunglasses. The main content area features the "YTview.com" logo and a list of services: YouTube Services, Facebook Services, Twitter Services, Instagram Services, Vimeo Services, Vine Services, SoundCloud Services, Pinterest Services, Google Services, SEO Services, Marketing Services, and Website Traffic. To the right of the services list is a cartoon character of a man with blonde hair. Below the services list, there is a navigation bar with links: Home | Update | Faq | Testimonials | Support. At the bottom, there is a copyright notice: "Copyright 2012 - 2015 © YTview. All rights reserved." and a PayPal logo.

100% Satisfaction Guaranteed

**YTview.com**

Your #1 Socials Media Provider  
Serving Over 50,000 Satisfy Clients!  
- Everyday Open 24/7/365 -  
LIVE 909287772 SERVICE DELIVERED

**WHY US?**

- YouTube Services
- Facebook Services
- Twitter Services
- Instagram Services
- Vimeo Services
- Vine Services
- SoundCloud Services
- Pinterest Services
- Google Services
- SEO Services
- Marketing Services
- Website Traffic

Home | Update | Faq | Testimonials | Support

Copyright 2012 - 2015 © YTview  
All rights reserved.

PayPal

VEVO  
UNIVERSAL  
UNIVERSAL MUSIC GROUP

SONY MUSIC



## Conclusion on digital frauds

- Advertisers lose a lot of money through fake YouTube views and other digital frauds.
- Google tries to filter this “invalid traffic” in order to not lose their credibility.
- How much trust should we – the people – put in what digital service providers tell us?



**Universität  
Zürich** UZH

**Institut für Informatik**

# Malware and (computer) trust



## Types of malware

- Computer viruses (or worms)
- Trojan horses (when for governments: (euphemistically) GovWare)
- Scareware
- Spyware
- Adware
- Ransomware



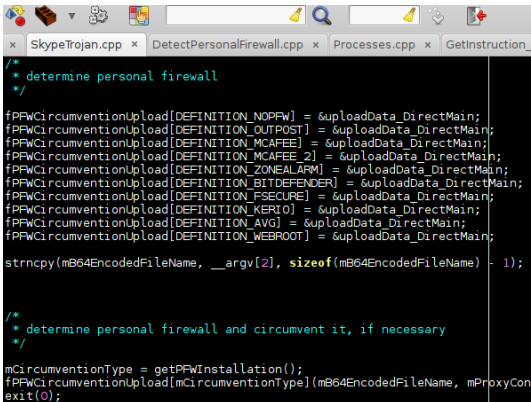
## Example: scareware business

- Software which scares users and creates incentives to carry out payments (e. g. to buy fake Anti-Virus (AV) software).
- Three main ways of infection
  - Social engineering
  - Drive-by downloads
  - Installation via botnets
- In an investigation (Stone-Gross et al. 2011) of three fake AV criminal networks, following figures emerged, for observation times of 3 months (AV1), 16 months (AV2) and 30 months (AV3):

Vendor	Prices	# infections	# sales	income/month
AV1	\$ 50–70	8.4 millions	189k	\$ 3 millions
AV2	\$ 50–90	6.6 millions	137k	\$ 313k
AV3	\$ 60–100	91.3 millions	1.97 millions	\$ 3.9 millions

## Example: Trojans / GovWare lowering IT security

Swiss Federal Department of the Environment, Transport, Energy and Communications (DETEC) created (disclosed) malware to intercept Skype calls (Mini-/MegaPanzer); showing e. g. ways to undermine IT security.



```
/*
 * determine personal firewall
 */

fPFWCircumventionUpload[DEFINITION_NOPFW] = &uploadData_DirectMain;
fPFWCircumventionUpload[DEFINITION_OUTPOST] = &uploadData_DirectMain;
fPFWCircumventionUpload[DEFINITION_MCAFEES] = &uploadData_DirectMain;
fPFWCircumventionUpload[DEFINITION_MCAFEES_2] = &uploadData_DirectMain;
fPFWCircumventionUpload[DEFINITION_ZONEALARM] = &uploadData_DirectMain;
fPFWCircumventionUpload[DEFINITION_BITDEFENDER] = &uploadData_DirectMain;
fPFWCircumventionUpload[DEFINITION_FSECURE] = &uploadData_DirectMain;
fPFWCircumventionUpload[DEFINITION_KERIO] = &uploadData_DirectMain;
fPFWCircumventionUpload[DEFINITION_AVG] = &uploadData_DirectMain;
fPFWCircumventionUpload[DEFINITION_WEBROOT] = &uploadData_DirectMain;

strcpy(mB64EncodedFileName, __argv[2], sizeof(mB64EncodedFileName) - 1);

/*
 * determine personal firewall and circumvent it, if necessary
 */

mCircumventionType = getPFWInstallation();
fPFWCircumventionUpload[mCircumventionType](mB64EncodedFileName, mProxyCon
exit(0);
```



## Example: Trojans / GovWare fabricating evidence

Hacking Team's Galileo Trojan Horse for Governments (GovWare) was leaked; showing e. g. ways to fabricate evidence.

```
https://github.com/hackedteam/rcs-common/blob/master/lib/rcs-common/evidence/file.rb#L17
Apps For quick access, place your bookmarks here on the bookmarks bar. Import bookmarks now... Other bookma

ELEM_DELIMITER = 0xABADC0DE

def content(*args)
  hash = [args].flatten.first || {}

  process = hash[:process] || ["Explorer.exe\\0", "Firefox.e
  process.encode!("US-ASCII")

  path = hash[:path] || ["C:\\Utenti\\pippo\\pedoporno.mpg"]
  path = path.to_utf16le_binary_null
```

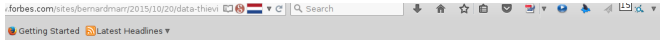


## How to trust trust?

- Pre-infected hardware (infected chips, firmware etc.)
- Pre-infected operating systems (system level backdoors)
- Backdoor-containing compilers
  - Cf. Karger & Shell (1974) on “Trap Door Insertion” describing boot level and compiler level backdoors.
  - Cf. Ken Thompson (1984) on “Reflections on Trusting Trust” describing a compiler level backdoor, inserting (and such preserving) itself when compiling future compiler versions.

## Example: Spyware appearing in App repositories

XcodeGhost: Manipulated Software Development Kits (SDKs) introduced malware into Apple's App Store (and Google Play).



### Apple Bans 100s Of iPhone Apps For Stealing Personal Data



**Bernard Marr**, CONTRIBUTOR

*I write about big data, analytics and enterprise performance*

[FOLLOW ON FORBES \(178\)](#)



Opinions expressed by Forbes Contributors are their own.

**FULL BIO** ▾

Apple announced yesterday that it had pulled hundreds of apps from its App Store because they violated the App Store's review process by collecting unapproved kit of data.

A third-party analytics service called [SourceDNA](#) discovered that apps using a [software developer kit \(SDK\) from a Chinese advertising platform called Youmi](#) were collecting personally identifiable data, including email addresses, Apple IDs,



**Universität  
Zürich** <sup>UZH</sup>

**Institut für Informatik**

**End**

## Questions & Comments?





## Discussion questions

- What are other possibilities to fake and distribute digital information?
- What are (further) possibilities to prove/check/detect the correctness of digital information?
- What is really provable by technology (trust/control over the technology), or: can a computer be trusted in general terms?