

# **16th IAP EUROPEAN REGIONAL CONFERENCE**

## **Handling of digital evidence and presenting it at court**

**Ivan Glavić**

**Tirana, 23 May 2017**



# TYPE OF DIGITAL EVIDENCE

- **HIDDEN DATA**
- **SOCIAL NETWORKS, FORUMS, P2P ...**
- **OPEN SOURCE DATA**

# TYPE OF DIGITAL EVIDENCE

- **SOCIAL NETWORKS, FORUMS, P2P ...**
- **OPEN SOURCE DATA**

# OPEN SOURCE DATA

- reliability of source
- accuracy of information
- relevance to the investigation
- legality of data (not obtained by excessive breachment of human rights)

ECHR (Copland v. UK, 2007) – right to privacy



# OPEN SOURCE DATA - EVIDENCE

**MUST BE RELIABLE, ACCURATE, RELEVANT,  
LEGAL**


- **computer data can be easily stored, searched, sorted and organised for trial**
- **can be acquired without the international legal assistance - Convention on cybercrime (Art. 32)**

*A Party may, without the authorisation of another party access publicly available (open source) stored computer data, regardless of where the data is located geographically*

- public registeries (land, company ...)
- WHOIS data (owner of an IP address or domain name)

# OPEN SOURCE DATA – OTHER PURPOSE

SHOULD BE AT LEAST LEGAL

- starting point for further investigative measures
  - detecting the potential suspects
  - locating a perpetrator
- 



Pentagon

East Potomac Park

East Potomac

Lady Bird Johnson Memorial Park

Jefferson Memorial

United States Holocaust Memorial Museum

Korean War Veterans Memorial

Lincoln Memorial

National Mall

Corcoran Gallery of Art

Freedom Plaza

Embassy of Bosnia and Herzegovina

World Bank

White House

School Without Walls

Embassy of Mexico

National City Christian Church

West End

Rose Park Recreation Center

Embassy Indonesia

Logan Circle Park

Mitchell Park

Oak Hill Cemetery

Dumbarton Oaks Park

California St NW

U St NW

Wisconsin Ave NW

Francis Playground

M St NW

Georgetown Waterfront Park

Theodore Roosevelt Island

George Washington Memorial Parkway

110

110

1

395

10B

10A

27

S Washington Blvd

N Jefferson Drive

14th St SW

7th St SW

11th St NW

9th St NW

7th St NW

6th St NW

Commercial Ave NW

Rock Creek and Potomac Pkwy NW

Kalorama Heights

Marie H Reed Recreation Center

U St NW

Card City

Rhode Isl

Rd NW

29

29

29

2

29

29

2

1

66

66

66

50

1

50

1

2

3

1

1

2

3

395

2

4

10B

10A

27

# FORENSIC ANALYSIS


## FEATURE > POSSIBLE ALLEGATIONS (BY DEFENCE)

- duration of process > failure to conduct search and seizure within the time limit on a court warrant
- data modification > evidence tampering / spoliation / destroying
- forensic software runs on keyword (combination, file extension...) search > withholding / hiding evidence




# FORENSIC ANALYSIS

## FEATURE > POSSIBLE ALLEGATIONS

- lacking of international standards > uncertainty of results
  - commercial origin of forensic software > partiality / dependence on police, prosecution
  - non disclosure due to protection of intellectual property rights > failure to provide transparency
- 

# FORENSIC ANALYSIS


## POSSIBLE ALLEGATIONS > SOLUTION

- **IMAGING (MIRRORING) PROCESS** = making the identical copy (forensic copy) of original data stored on a computer system + hash value
  - **HASH VALUE** = verification on the integrity of a copy
  - **(SECURITY COPY, BACKUP COPY, DEFENCE COPY)**
- 

# LEGAL IMPLICATION OF IMAGING PROCESS

- dividing the stage of search and seizure from subsequent forensic analysis
  - search and seizure = collecting the device + imaging process (acquiring the data)*
  - time limit on the search warrant*
  - signing the minutes by defendant*

# LEGAL IMPLICATION OF IMAGING PROCESS

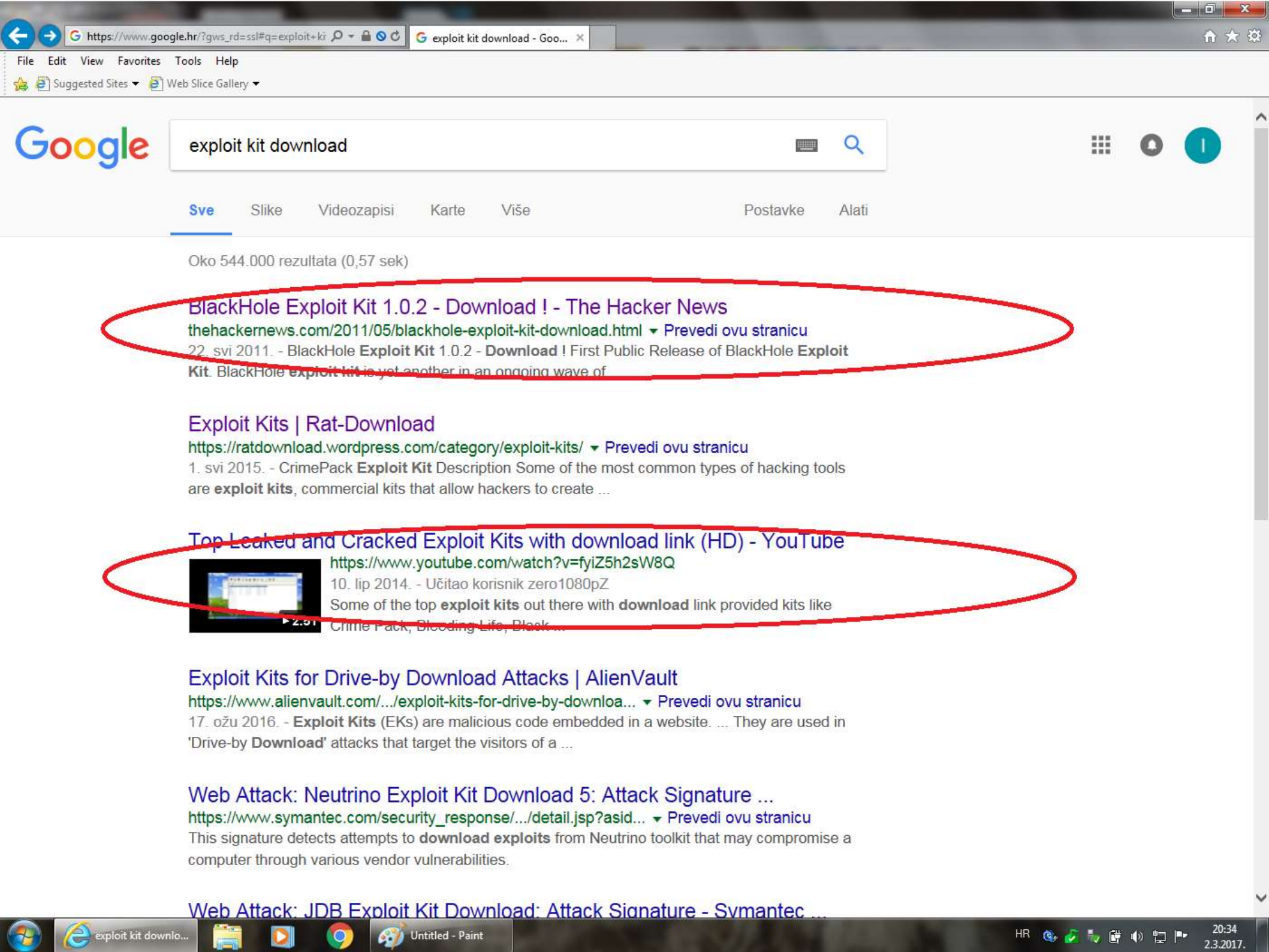
- dividing the stage of search and seizure from subsequent forensic analysis
  - protection of the right to a fair trial (equality of arms, right to challenge incriminating evidence)
  - possibility to repeat the analysis
  - possibility to leave in possession / return computer device to the rightful owner (victim!)
- 

# EXEMPTION FROM IMAGING PROCESS

- **REAL-TIME MEASURES**
  - search and seizure on working computer, prior to turning off and taking device
  - data interception
- observing and real-time recording of computer process (data creation, modification, erasure) instead of stored data

# COMPUTER USED BY MORE PERSONS

- difficulty to identify the perpetrator on the level of computer skills



exploit kit download

Sve Slike Videozapisi Karte Više Postavke Alati

Oko 544.000 rezultata (0,57 sek)

### BlackHole Exploit Kit 1.0.2 - Download ! - The Hacker News

[thehackernews.com/2011/05/blackhole-exploit-kit-download.html](http://thehackernews.com/2011/05/blackhole-exploit-kit-download.html) ▾ Prevedi ovu stranicu

22. svi 2011. - BlackHole **Exploit Kit 1.0.2 - Download !** First Public Release of BlackHole **Exploit Kit**. BlackHole **exploit kit** is yet another in an ongoing wave of

### Exploit Kits | Rat-Download

<https://ratdownload.wordpress.com/category/exploit-kits/> ▾ Prevedi ovu stranicu

1. svi 2015. - CrimePack **Exploit Kit** Description Some of the most common types of hacking tools are **exploit kits**, commercial kits that allow hackers to create ...

### Top Leaked and Cracked Exploit Kits with download link (HD) - YouTube



<https://www.youtube.com/watch?v=fyiZ5h2sW8Q>

10. lip 2014. - Učitao korisnik zero1080pZ

Some of the top **exploit kits** out there with **download** link provided kits like Crime Pack, Bleeding Life, Black ...

### Exploit Kits for Drive-by Download Attacks | AlienVault

<https://www.alienvault.com/.../exploit-kits-for-drive-by-downloa...> ▾ Prevedi ovu stranicu

17. ožu 2016. - **Exploit Kits** (EKs) are malicious code embedded in a website. ... They are used in 'Drive-by **Download**' attacks that target the visitors of a ...

### Web Attack: Neutrino Exploit Kit Download 5: Attack Signature ...

[https://www.symantec.com/security\\_response/.../detail.jsp?asid...](https://www.symantec.com/security_response/.../detail.jsp?asid...) ▾ Prevedi ovu stranicu

This signature detects attempts to **download exploits** from Neutrino toolkit that may compromise a computer through various vendor vulnerabilities.

### Web Attack: JDB Exploit Kit Download: Attack Signature - Svmantec ...

# Hackforums.net

06-12-2016, 02:11 AM (This post was last modified: 11-07-2016 11:56 AM by Roshke.)



**Roshke**

Knowledge is power, power corrupts.



Hello, I am selling **VPS** and **Dedicated Servers**.

### **What is allowed on these servers?**

IP Spoofing(DDoS), VPNs, DMCA, Scanning(Only with our Blacklist) content and pretty much anything that else you want to do that is not listed in the not allowed list.

### **What is NOT allowed on these servers?**

Abusing Cores(VPS only), Child Porn, Anti-Government sites, Spamming(Mass mailing etc...), Botnet controllers, Bruteforce, Scanning government ranges.

### **How long does it take to setup my server?**

All orders are reviewed manually and can take up to 24 - 48 hours

### **What payment methods do you accept?**

At the moment Bitcoins only, Paypal will be soon.

### **Do you offer refunds?**

Only if the product was undelivered then you have the right to request a refund.

## Prices

### KVM VPS

**\$15**/month

1 Intel E5 CPU Core

25 GB HDD


1 GB RAM

1 Gbit/s Port (Unmetered)

24/7 Support



# COMPUTER USED BY MORE PERSONS

- difficulty to identify the perpetrator on the level of computer skills
  - computers can be remoted from distance
  - computer process can be programmed in advance
  - computer may be controlled without a knowledge of the rightful owner (bot)
- 

# COMPUTER USED BY MORE PERSONS

- Computer forensics must be combined with a "classic" evidence, such as:
  - *evidence on suspect's whereabouts (record on entering the country, cameras...)*
  - *"money trail", financial transactions*

# REPRESENTING THE CASE BEFORE COURT

- **Knowledge on informatics is important**
- **Knowledge on how to make it simple is crucial**
  - *appeal court, constitutional court, ECHR ...*
  - *reasoning decisions must be understandable to public, "ordinary" people (public scrutiny, building confidence in judiciary system)*

# REPRESENTING THE CASE BEFORE COURT

- **MAKING IT SIMPLE:**
  - **avoid abbreviations** (ISP, DoS, IP address...)
  - **focus on the end result**, not on the process of forensic analysis
  - **rely on** (police, court) **expert**
  - **compare a cybercrime to correspondent „classic“ , „traditional“ , „real-life“ crime**

# REPRESENTING THE CASE BEFORE COURT

<b>CYBER</b>	<b>"REAL-LIFE"</b>
<b>hash value</b>	<b>fingerprint</b>
<b>digital forensics</b>	<b>financial expertise</b>
<b>data interception</b>	<b>telephone surveillance</b>
<b>electronic evidence</b>	<b>document</b>
<b>imaging process</b>	<b>verified copy</b>

# REPRESENTING THE CASE BEFORE COURT

<b>CYBERCRIME</b>	<b>"CLASSIC" CRIME</b>	<b>PROTECTED VALUE</b>
<b>illegal access</b>	<b>home invasion, burglary</b>	<b>integrity (of data, home)</b>
<b>illegal interception</b>	<b>eavesdropping</b>	<b>privacy of communication</b>
<b>data interference</b>	<b>property destroying</b>	<b>property</b>
<b>computer forgery</b>	<b>forgery</b>	<b>authenticity (of data, document)</b>
<b>computer fraud</b>	<b>fraud</b>	<b>property</b>

# REPRESENTING THE CASE BEFORE COURT

## DEALING WITH USUAL DEFENCES:

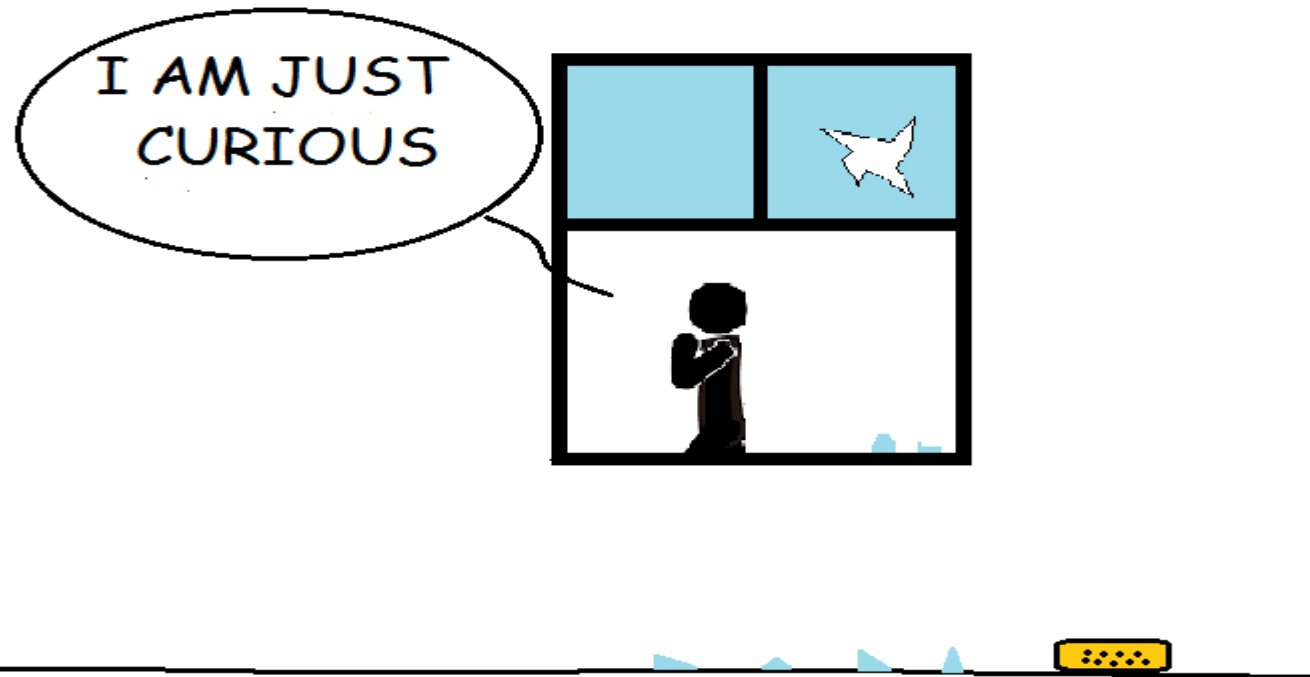
"I wasn't doing any harm to anyone"

"I just wanted to find out how does a malware work"

"I was checking the vulnerability / weakness of computer system"

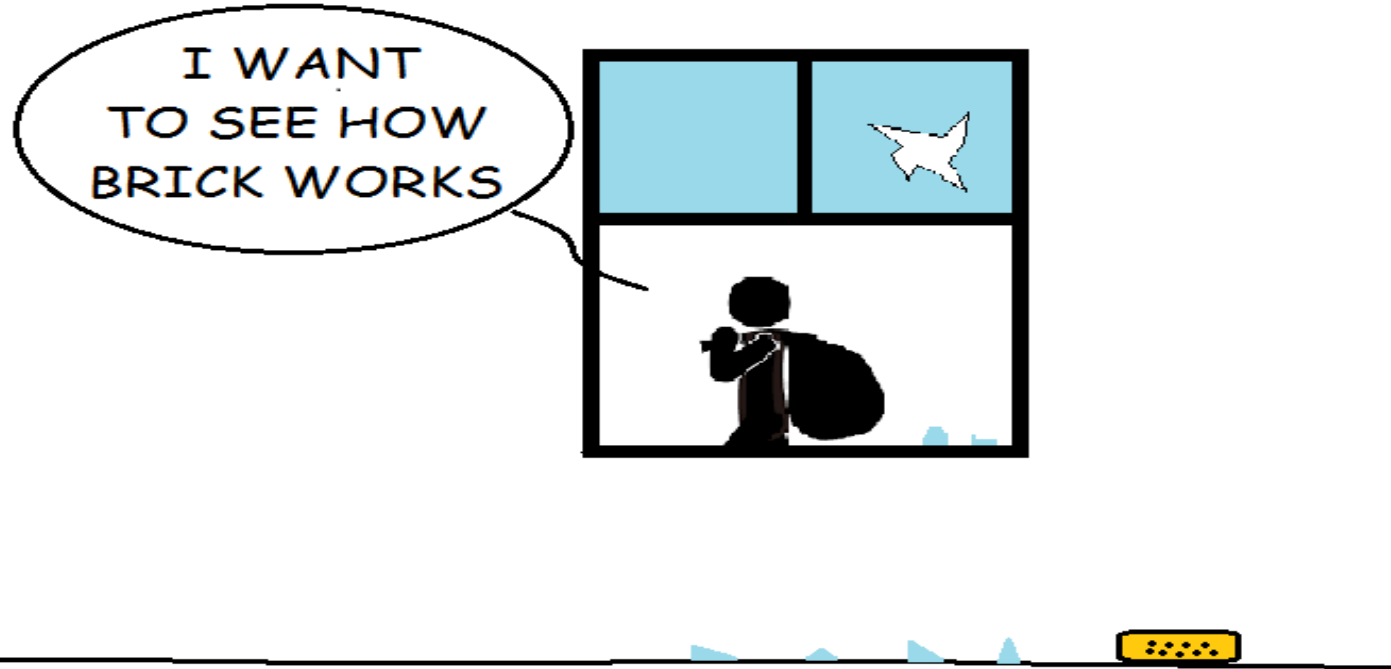
"Possessing a computer program is not illegal"

"I wasn't doing any harm to anyone"

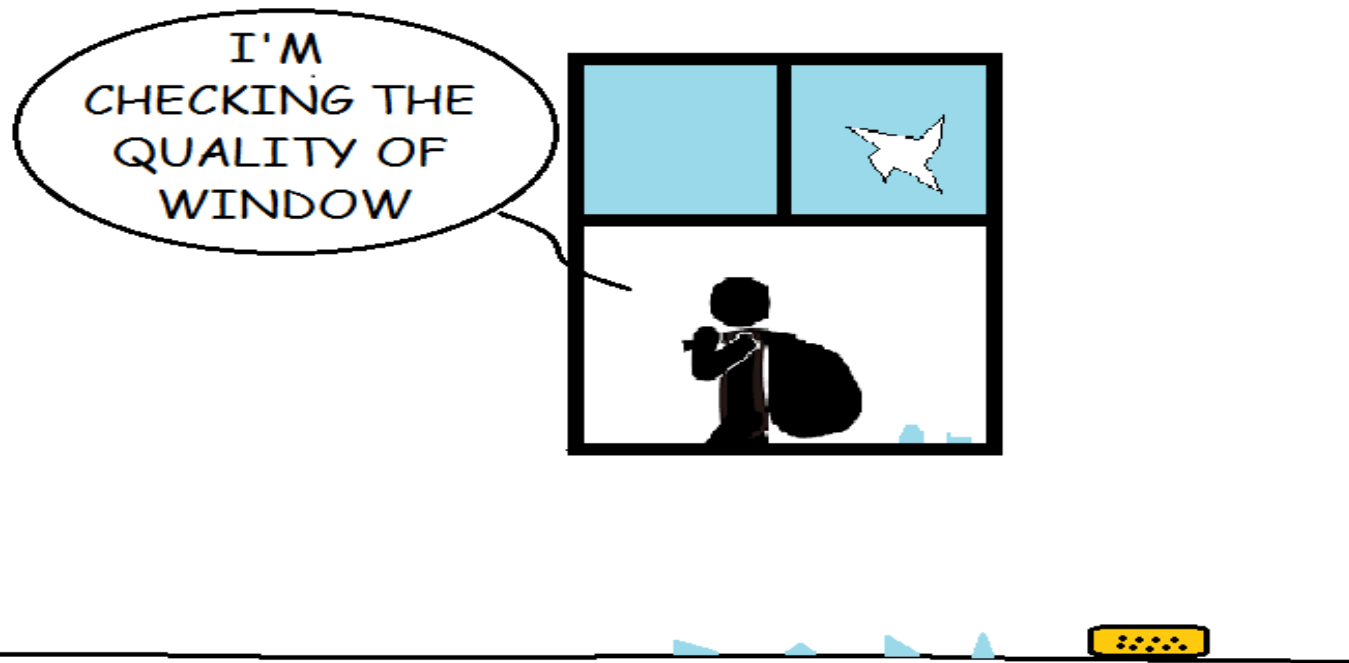




"I just wanted to find out how  
does a malware work"



"I was checking the vulnerability of computer system"



# "Possessing a computer program is not illegal"





PARENTAL CONTROL SOFTWARE

Sve Slike Videozapisi Knjige Karte Više Postavke Alati

Oko 1.510.000 rezultata (0,84 sek)

### The Best Parental Control Software of 2017 | PCMag.com

[www.pcmag.com/article2/0,2817,2346997,00.asp](http://www.pcmag.com/article2/0,2817,2346997,00.asp) ▾ Prevedi ovu stranicu  
Parenting styles run the gamut, and so do the features available in **parental control** and **monitoring** utilities. We'll help you pick the service that's right for your ...  
ContentWatch Net Nanny 7 - Kaspersky Safe Kids - Symantec Norton Family Premier

### The best free parental control software 2017 | TechRadar

[www.techradar.com/news/the-best-free-parental-control-software](http://www.techradar.com/news/the-best-free-parental-control-software) ▾ Prevedi ovu stranicu  
Prije 6 dana - **Parental control** suites including content filters, keyloggers and **monitoring** tools to help keep your kids safe online.

### Best Free Parental Control Software for PC, Mac, iOS, Android | Digital ...

[www.digitaltrends.com](http://www.digitaltrends.com) › Computing ▾ Prevedi ovu stranicu  
24. srp 2016. - The Internet can be a dangerous place. Check out our top picks for the best free **parental control software**, so you can block and monitor the ...

### Best Parental Time Control Software Review - Top Ten Reviews

[www.toptenreviews.com](http://www.toptenreviews.com) › Software ▾ Prevedi ovu stranicu  
25. lis 2016. - **Parental time control software** will keep kids safe, on task and out of trouble.  
**Parental time control software** performs two functions. It **controls** ...

### Qustodio: Best Parental Control Software

<https://www.qustodio.com/> ▾ Prevedi ovu stranicu  
Free **parental control software**. Monitor and track your child's online activity. Block dangerous sites and protect kids from online bullying.



EMPLOYEE MONITORING SOFTWARE



Sve Slike Videozapisi Karte Više Postavke Alati

Oko 1.150.000 rezultata (0,65 sek)

### Employee Monitoring Software - Live Screens, Web / Apps, More

[Oglas](#) [www.teramind.co/Employee/Monitoring](http://www.teramind.co/Employee/Monitoring) +1 212-603-9617  
Ranked Most Advanced **Employee Monitoring** Solution. Cloud or On-Premises.  
Hidden Mode Available. · Avoid Insider User Risk. · Increase Productivity · Screen/Files/Printed Docs  
Services: Insider Risk Prevention, User Activity Monitoring, Cloud or On-Premises, Live & Recorde...  
Visual Screen Recording      Investigate Employees  
User Activity Logs              Productivity Analysis

### SolarWinds® NPM 12 - On-Prem, Cloud & Hybrid Visibility

[Oglas](#) [www.solarwinds.com/NPMv12](http://www.solarwinds.com/NPMv12)  
Full Feature 30 Free Trial  
Services: Traffic Categories, Traffic Classification, Packet Analysis Sensors, Application Dashboard  
SolarWinds Home · Software Downloads · Network Performance Mgmt. · Server & App Monitoring

### Employee Monitoring Tool - Try It Now for Free - balabit.com

[Oglas](#) [www.balabit.com/](http://www.balabit.com/)  
Granular Control of Remote Access  
Enterprise Class · Lower Forensics Costs · High Availability · High Quality Audit · Easy-to-use GUI  
Evaluation Version · Support · Features · Pricing

### The Best Employee Monitoring Software of 2017 - Top Ten Reviews

[www.toptenreviews.com/.../software/best-employee-monitoring-s...](http://www.toptenreviews.com/.../software/best-employee-monitoring-s...) Prevedi ovu stranicu  
9. sij 2017. - We rank the best **employee monitoring software** with side-by-side comparisons. Read  
in-depth reviews and articles regarding PC monitoring.  
Teramind · SentryPC · Veriato 360 · StaffCop



CHEATING SPOUSES MONITORING



Sve Slike Videozapisi Karte Više Postavke Alati

Oko 578.000 rezultata (0,41 sek)

### Spytech's Spouse Monitoring Software - Catch a cheating spouse and ...

<https://www.spytech-web.com/spouse-monitoring.shtml> ▾ Prevedi ovu stranicu  
**Spouse Monitoring** Reinforce and restore trust and faithfulness in your **marriage!** Do you suspect your **spouse** is **cheating** on you? Do they have an addiction to ...

### Best Spouse Monitoring Software of 2017 | Top Ten Reviews

[www.toptenreviews.com](http://www.toptenreviews.com) > [Software](#) > [Privacy](#) ▾ Prevedi ovu stranicu  
While it might be tempting to use **spouse monitoring** software to catch a **cheating husband** or **wife**, we strongly recommend against it. In many states it is legal to ...

### Cheating Spouse GPS Tracking - Truth About Deception

<https://www.truthaboutdeception.com/gps-tracking.html> ▾ Prevedi ovu stranicu  
Buy **GPS tracking** to catch a **cheating spouse**. ... Are you thinking about using a GPS device to **monitor** your **spouse**? If so, please consider the following: if you ...

### 11 Spy Gadgets to Help Keep Tabs on Your Cheating Spouse (list)

[www.gadgetreview.com](http://www.gadgetreview.com) > ... > [Cheating Spouses](#) ▾ Prevedi ovu stranicu  
21. lip 2016. - 11 Spy Gadgets to Help Keep Tabs on Your **Cheating Spouse** (list) ... If you feel that your **spouse** might be **cheating** on you and you're not sure .... Gadgets for real spies)) I think it's easiest to **monitor** mobile phone, there is all ...

### Is Your Spouse Cheating? Spy On Their Cell Phone To Find Out ...

<https://www.flexispy.com/.../catch-cheating-spouse-cell-phone.ht...> ▾ Prevedi ovu stranicu  
How A Cell Phone Can Point To A **Cheating Spouse**. They are jumpy when ... FlexiSPY Gives You Complete **Monitoring** Control Of Your **Spouse's** Cell Phone.



CHEATING SPOUSES MONITORING

Sve Slike Videozapisi Karte Više Postavke Alati

Oko 580.000 rezultata (0,63 sek)

### Spytech's Spouse Monitoring Software - Catch a cheating spouse and ...

[https://www.spytech-web.com/spouse-monitoring.shtml](#) Prevedi ovu stranicu  
**Spouse Monitoring** Reinforce and restore trust and faithfulness in your **marriage!** Do you suspect your spouse is cheating on you? Do they have an addiction to ...  
Posjetili ste ovu stranicu 01.03.17..

### Best Spouse Monitoring Software of 2017 | Top Ten Reviews

[www.toptenreviews.com](#) > Software > Privacy > Prevedi ovu stranicu  
While it might be tempting to use **spouse monitoring** software to catch a **cheating husband** or **wife**, we strongly recommend against it. In many states it is legal to ...

### Cheating Spouse GPS Tracking - Truth About Deception

[https://www.truthaboutdeception.com/gps-tracking.html](#) > Prevedi ovu stranicu  
Buy GPS **tracking** to catch a **cheating spouse**. ... Are you thinking about using a GPS device to **monitor** your **spouse**? If so, please consider the following: if you ...

### Is Your Spouse Cheating? Spy On Their Cell Phone To Find Out ...

[https://www.flexispy.com/.../catch-cheating-spouse-cell-phone.ht...](#) > Prevedi ovu stranicu  
How A Cell Phone Can Point To A **Cheating Spouse**. They are jumpy when ... FlexiSPY Gives You Complete **Monitoring** Control Of Your **Spouse's** Cell Phone.

### 3 Ways to Catch Your Cheating Spouse - wikiHow

[www.wikihow.com](#) > ... > Married Life > Cheating Spouses > Prevedi ovu stranicu  
If you really believe your **spouse** is **cheating** on you, yet after **monitoring** phone calls, emails, and travel details, all you have is a gut feeling, than you need to ...

### How can i spy on my husband cell phone without touching his cell

**THE END**