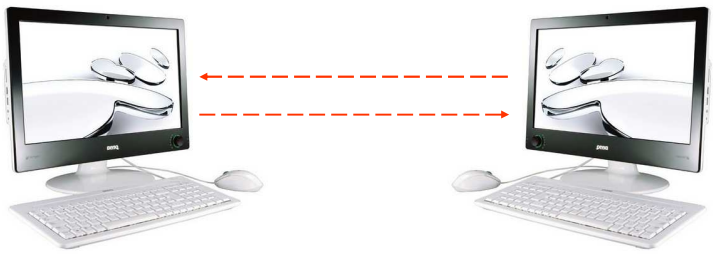
Problematiky odhaľovania počítačovej kriminality v trestnom konaní

Prezídium Policajného zboru
Úrad kriminálnej polície
Odbor počítačovej kriminality

mjr. JUDr. Zoltán Šťavnický
kpt. Mgr. Marek Švarc

Čo je počítačová sieť?

Počítačová sieť je sústava najmenej dvoch vzájomne prepojených počítačov vytvorená za účelom komunikácie a zdieľania sieťových prostriedkov.



Prehľad počítačových sietí

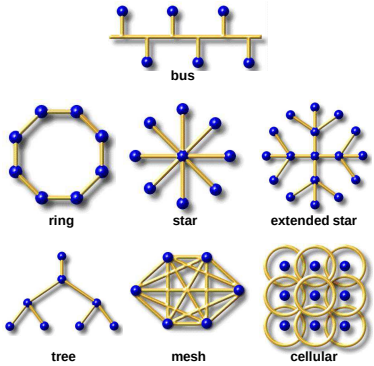
Počítačové siete je možné rozdeliť na základe:

- fyzickej topológie;
- logickej topológie;
- metódy pripojenia;
- veľkosti;
- funkčnosti.

Prehľad počítačových sietí

Počítačové siete je možné rozdeliť na základe:

- fyzickej topológie;



Prehľad počítačových sietí

Počítačové siete je možné rozdeliť na základe:

- metódy pripojenia;

pripojenie káblom (wired connection)

pripojenie bez kábla (wireless connection)

Prehľad počítačových sietí

Počítačové siete je možné rozdeliť na základe:

- veľkosti;

Základné typy:

PAN - veľmi malá osobná sieť. Spolupracujúce zariadenia obvykle slúžia len jednej osobe (typicky prepojenie mobilu a počítača, PDA, notebooku)

Prehľad počítačových sietí

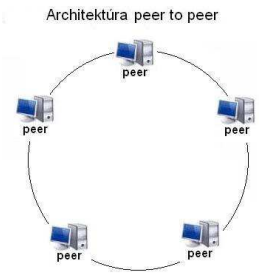
LAN - lokálna počítačová sieť. Spájajú uzly (počítače) v rámci malého územia, resp. v rámci jednej budovy rádovo do vzdialenosti sto metrov. Slúžia hlavne pre zdieľanie dát a zdrojov (zariadení) v rámci jednej firmy, budovy, lokality

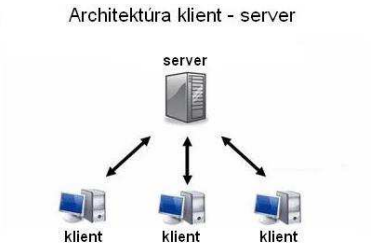
WAN - rozsiahla sieť. Spája rôzne LAN siete v pôsobnosti krajín, kontinentov ale i sveta

Prehľad počítačových sietí

Počítačové siete je možné rozdeliť na základe:

- funkčnosti.





Sieťové zariadenia

- Hub;
- Switch;
- Router;
- Modem;
- Firewall;
- Gateway.

Hub

- pripája zariadenia k počítačovej sieti;
- pracuje s dátami usporiadanými do frames (dátových rámcov);
- každý frame rozposiela na všetky porty – tzv. „broadcasting“

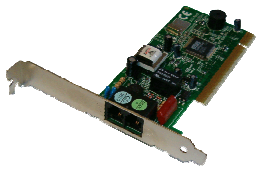
Switch

- pripája zariadenia k počítačovej sieti;
- pracuje s dátami usporiadanými do frames (dátových rámcov);
- inteligentnejší ako hub;
- vnútorná pamäť, v ktorej sú uchované všetky MAC pripojených PC.

Router

- spracováva data packets (dátové pakety);
- hlavná úloha - smerovanie packetov do inej počítačovej siete;
- väčšinou prepája dve alebo viac sietí;
- smerovanie - pomocou hlavičky paketu a „forwardovacej tabuľky“;
- komunikácia medzi dvoma routerami - cez ICMP protokol (Internet Control Message Protocol);
- dnešné routre často naviac obsahujú: switch (4-8 port), NAT (network address translation) , DHCP server, DNS proxy server, hardware firewall.

Modem

- zariadenie na prevod analógového singnálu na digitálny a naopak;
- názov vznikol spojením dvoch slov: **mod**ulátor a **dem**odulátor;
- **Modulácia** je konvertovanie signálu z odosielajúceho PC do analógovej podoby pre analógovú linku. Na druhej strane ide o konvertovanie analógového signálu do digitálnej podoby.
- komunikácia môže prebiehať cez telefónnu linku, cez rozvod káblovej televízie, cez rádiový prenos;
- modemy sa delia na interné a externé;
- **Interné** – pripojené cez PCI, AMR,CMR;
- **Externé** – pripojené cez porty COM1, COM2, USB, RJ-45;
- ISDN adaptér - Integrated Services Digital Network ;
- ISDN – digitálna linka, ktorá využíva na prenos dva kanály (channel B, channel D);
- kanál B – prenos samotnej informácie s prenosovou rýchlosťou 64 kbps;
- kanál D – signalizácia a prenos riadiacich informácii medzi ISDN ústredňou a komunikačným zariadením.

Firewall


- hardware;
- software;
- vytvára tzv. „ohnivú stenu“ medzi internetom a počítačovou sieťou;
- účel – oddelenie LAN od internetu, kontrola dátového toku medzi týmito sieťami;
- dátový tok je kontrolovaný na základe definovaných pravidiel a podmienok, ku ktorým prislúcha následná akcia;
- dve základné akcie sú "povoliť dátový tok" a "zamietnuť dátový tok“;

Fyzické pripojenie

MAC adresa

- Media Access Control
- Komunikácia cez ARP (Address Resolution Protocol)
- Unikátne číslo pevne zakódované do sieťovej karty
- 6 dvojíc hexadecimálnych znakov oddelených pomlčkami

MAC adresa

- Každý sieťový adaptér (sieťová karta) má zaručenú jedinečnú MAC adresu. Jedinečnosť prvých 6 hexadecimálnych znakov (ID výrobcu) zaručuje IEEE, jedinečnosť posledných 6 zabezpečujú jednotliví výrobcovia.
- http://standards.ieee.org/regauth/oui/oui.txt

00-21-6A-6B-42-FC

Kód výrobcu

IP adresa

- prostriedok na identifikáciu PC na sieti;
- 4 čísla oddelené bodkami:

213.81.171.100

- Minimálna IP - 0.0.0.0
- Maximálna IP - 255.255.255.255
- Maximum IP adries je 4,294,967,296
- Tento problém rieši IP v6

IP v6

- Na rozdiel od IP v4 (4 miliardy IP) podporuje 2^{128} IP adries (340 sextiliónov);
- osem skupín po štyroch hexadecimálnych čísliciach oddelených dvojbodkou :

2001:0db8:85a3:08d3:1319:8a2e:0370:7334

- ak skupina štyroch číslic obsahuje 0000, je možné ju vynechať;

Domény

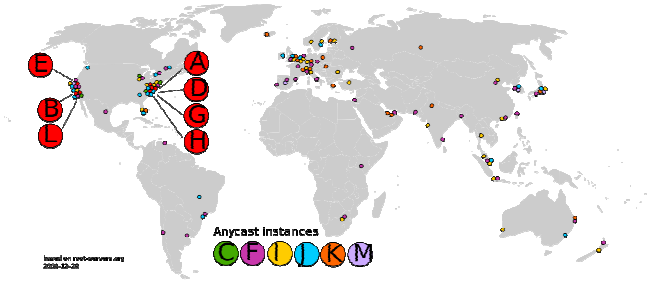
- Doména nahrádza nutnosť pamätať si IP adresu;
- Doména najvyššej úrovne (top-level domain; skratka TLD) je posledná časť plne kvalifikovaného názvu domény (za poslednou bodkou);
- Internet Assigned Numbers Authority (IANA);
- Rozdelenie domén:
  - **TLD kód krajiny (ccTLD)** – používané pre jednotlivé krajiny alebo závislé územia. Majú 2 písmená,
    napr. .sk pre Slovensko;
  - **všeobecné TLD (gTLD)** – určené pre použitie určených tried organizácií, napr.:
    - .com (*commercial*) pre komerčné organizácie ;
    - .org (*organisation*) - neziskové organizácie;
    - .biz (*business*) - obchodná doména;
    - .info (*information*) – informácie;
    - .name (*name*) - mená osôb;
    - .mil (military) – vojenské;
    - .gov (governement) – vládne – hlavne USA;
  - **Infraštruktúrne TLD** napr.:
    - .arpa - United States Department of Defense Advanced Research Projects Agency;
    - .root

www.pobocka.firma.azet.sk

(Príklad domény)

DNS

- Domain Name Server;
- Ukladá prístup k informácii o názve stroja (hostname) a názve domény v istej distribuovanej databáze v internete;
- Na svete existuje 13 hlavných DNS:

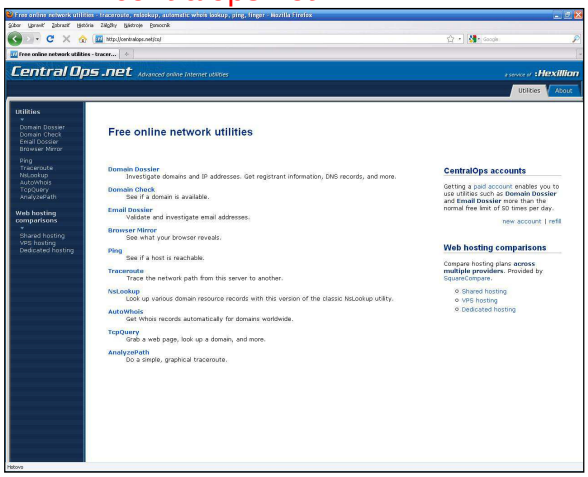


- Anycast z dôvodu IPv6 – z dôvodu obmedzeného prenosu – 512 bytov UDP;
- Address DNS Lookup;
- Reverse DNS Lookup;

213.215.107.250 = azet.sk

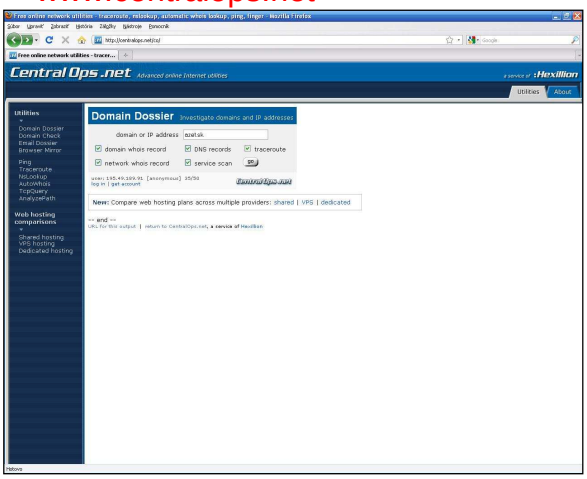
Preverovanie domén a IP adries

- www.centralops.net



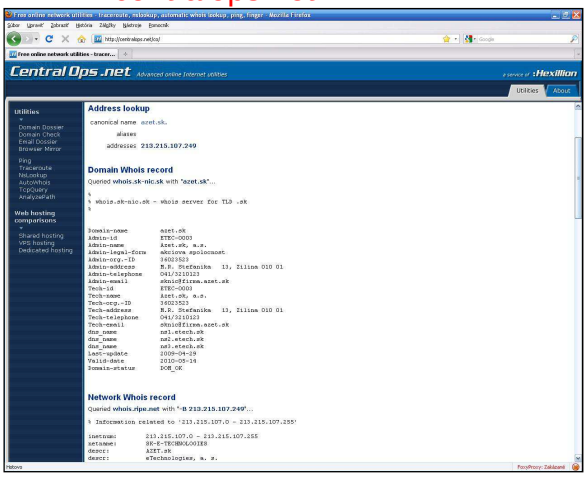
Preverovanie domén a IP adries

- www.centralops.net



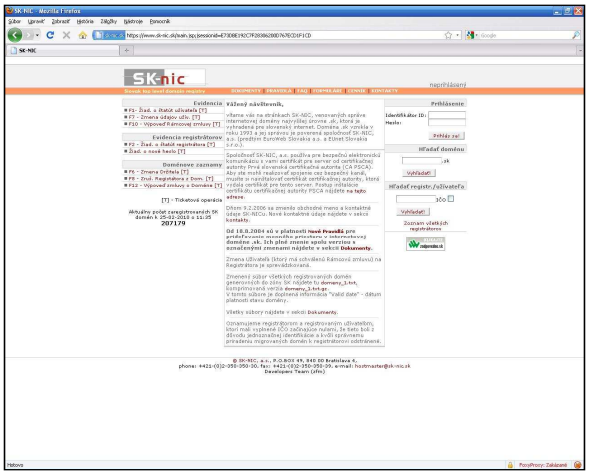
Preverovanie domén a IP adries

- www.centralops.net



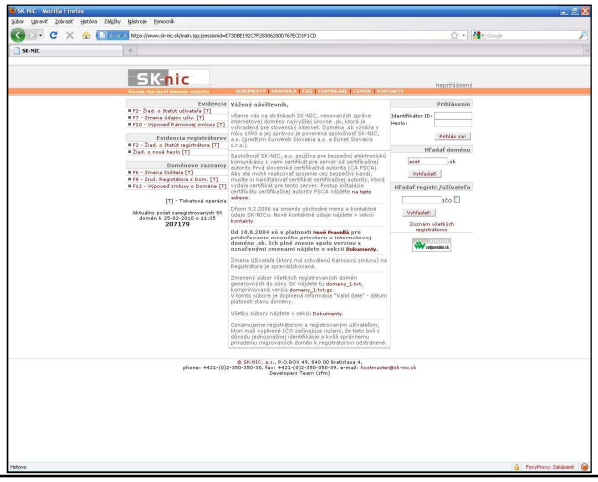
Preverovanie slovenských domén

- www.sk-nic.sk



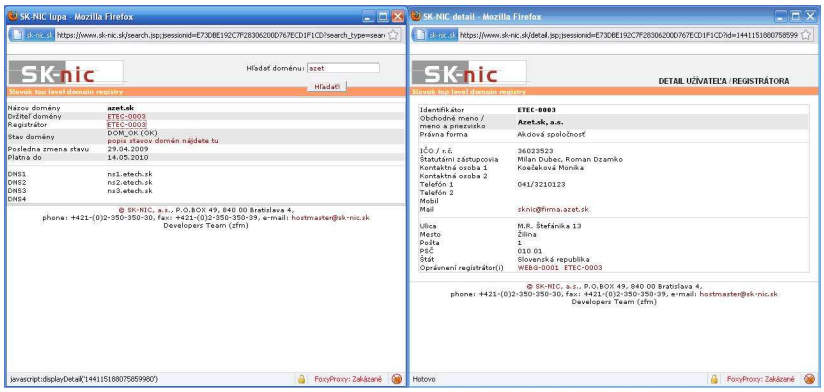
Preverovanie slovenských domén

- www.sk-nic.sk



Preverovanie slovenských domén

- www.sk-nic.sk



PC a porty

- procesy spustené na PC počúvajú prichádzajúce pripojenia
- IP adresy identifikujú PC a porty identifikujú software spustený na PC
- Celkovo je 65535 TCP and 65535 UDP portov
- Najviac využívané porty sú od 1 to 1024

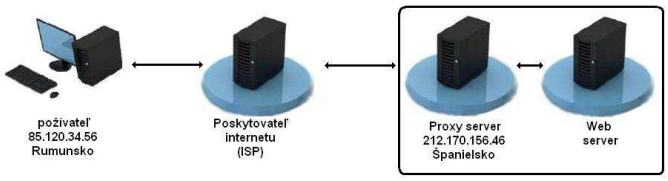
Anonymný prístup na internet

- nie je mýtus;
- čoraz väčší počet prípadov, pri ktorých je použitý;

Proxy

- Druh anonymizéra;
- Umožňuje klientom nepriame pripojenie k inému serveru;
- proxy server funguje ako sprostredkovateľ medzi klientom a cieľovým serverom;
- prekladá požiadavky klienta a oproti cieľovému serveru vystupuje ako klient;
- prijatú požiadavku potom odosiela naspäť klientovi;
- Hardware;
- Software.

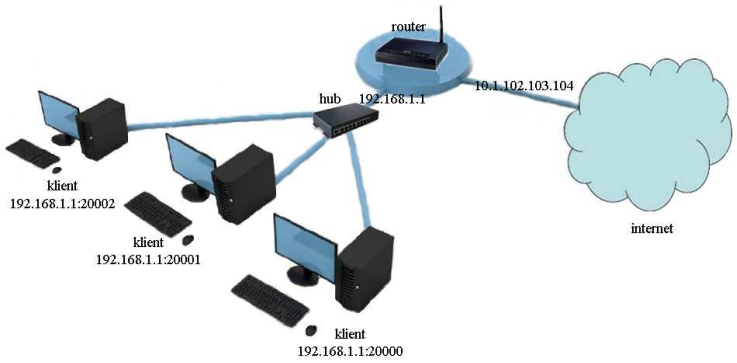
Proxy (anonymizačné)



NAT

- Network Address Translation;
- proces zmeny informácie o sieťovej adrese v datagrame hlavičky paketov;
- dnes sa často používa v spojení so sieťovou maškarádou (network masquerading) alebo IP maškarádou (IP masquerading);
- skladá sa z adries privátnej siete ukryté za jedinú IP adresu;
- mechanizmus býva väčšinou implementovaný v routeri;
- využíva prekladovú tabuľku.

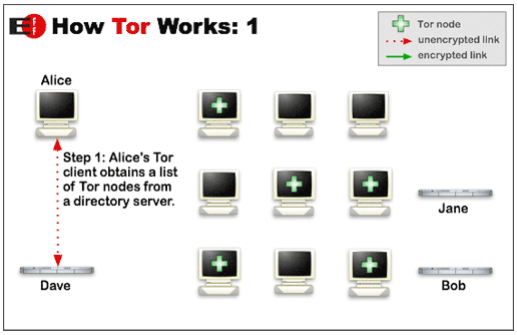
NAT



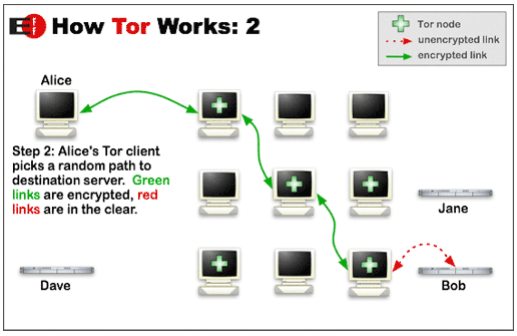
TOR

- Druh anonymizéra;
- sieť virtuálnych tunelov, ktoré zabezpečujú súkromie a bezpečnosť na internete;
- dátový tok je distribuovaný cez niekoľko miest (bodov) na internete;
- žiadny bod sa nemôžu pripojiť do cieľa
- obtiažne sledovateľný;
- po spojení maže stopy;
- jediná možnosť odhalenia uzla siete TOR (páchateľa) je analyzovať celý jeho dátový tok.
- http://www.torproject.org/
- nakonfigurovaný pre Firefox.

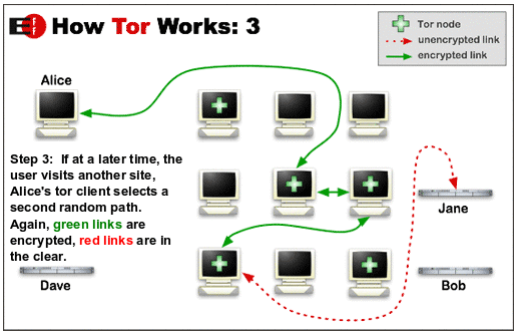
TOR


How Tor Works: 1
Tor node
unencrypted link
encrypted link
Alice
Step 1: Alice's Tor client obtains a list of Tor nodes from a directory server.
Jane
Dave
Bob

TOR


How Tor Works: 2
Tor node
unencrypted link
encrypted link
Alice
Step 2: Alice's Tor client picks a random path to destination server. Green links are encrypted, red links are in the clear.
Jane
Dave
Bob

TOR



Služby obsiahnuté v internete

- Elektronická pošta (e-mail),
- Diskusné skupiny (Usenet),
- Telnet,
- FTP (File Transfer Protocol),
- IRC (Internet Relay Chat),
- WWW (World Wide Web),
- P2P siete (Peer to peer),
- VOIP

E-mail - definícia

- Servis, ktorý umožňuje posielať:
  - správy;
  - súbory;
- Možnosť odosielať e-mail:
  - od 1 korešpondenta k 1 korešpondentovi;
  - od 1 korešpondenta k ∞ korešpondentom;
- Adresovateľný cez počítačovú sieť;

Formát e-mailu

mojemeno@mojmail.sk

- Príklad: jozko.mrkvicka@minv.sk
- Povolené: bodka, podtržník, čísla
- Nepovolené: medzery, špeciálne znaky, diakritika

Identifikácia IP adresy z hlavičky elektronickej pošty

Delivered-To: radoslav.lefcik@gmail.com
Received: by 10.100.148.11 with SMTP id v11cs73606and;
Mon, 13 Sep 2010 05:36:33 -0700 (PDT)
Received: by 10.204.102.68 with SMTP id f4mr3192368bko.30.1284381391626;
Mon, 13 Sep 2010 05:36:31 -0700 (PDT)
Return-Path: <peter.takac@minv.sk>
Received: from mail2.minv.sk (mail2.minv.sk [213.81.171.179])
by mx.google.com with SMTP id k15si14092226bkb.81.2010.09.13.05.36.28;
Mon, 13 Sep 2010 05:36:31 -0700 (PDT)
Received-SPF: pass (google.com: domain of peter.takac@minv.sk designates 213.81.171.179 as permitted sender) client-ip=213.81.171.179;
Authentication-Results: mx.google.com; spf=pass (google.com: domain of peter.takac@minv.sk designates 213.81.171.179 as permitted sender) smtp.mail=peter.takac@minv.sk
Received: (qmail 471 invoked by uid 504); 13 Sep 2010 12:36:44 -0000
Received: from 10.33.10.30 by mailbaout (envelope-from <peter.takac@minv.sk>, uid 501) with qmail-scanner-1.25
(clamdscan: 0.96.2/11896.
Clear:RC:0(10.33.10.30):.
Processed in 0.071434 secs); 13 Sep 2010 12:36:44 -0000
Received: from unknown (HELO mailba.minv.sk) (10.33.10.30)
by mail.minv.sk with SMTP; 13 Sep 2010 12:36:44 -0000
Received: (qmail 4623 invoked by uid 28956); 13 Sep 2010 12:36:27 -0000
Delivered-To: radoslav.lefcik@minv.sk
Received: (qmail 4471 invoked by uid 100); 13 Sep 2010 12:36:12 -0000
Received: from unknown (HELO mail2.minv.sk) (10.33.10.34)
by mailba.minv.sk with SMTP; 13 Sep 2010 12:36:12 -0000
Received: (qmail 374 invoked by uid 504); 13 Sep 2010 12:36:23 -0000
Received: from 10.33.12.148 by mailbaout (envelope-from <peter.takac@minv.sk>, uid 501) with qmail-scanner-1.25
(clamdscan: 0.96.2/11896.
Clear:RC:0(10.33.12.148):.
Processed in 0.069147 secs); 13 Sep 2010 12:36:23 -0000
Received: from unknown (HELO OKP004Takac) (10.33.12.148)
by mail.minv.sk with SMTP; 13 Sep 2010 12:36:22 -0000
From: =?iso-8859-2?B?UGV0ZXIgVGFr4eg=?= <peter.takac@minv.sk>
To: "'rado lefcik'" <radoslav.lefcik@minv.sk>,
Subject:
X-Eset-AntiSpam: OK;50;calc;2010-09-16 14:16:52;1009161416520001;BEA8
Date: Mon, 13 Sep 2010 14:38:05 +0200
Message-ID: <810E95AFEE014904912CBE01BDCC5A54@OKP004Takac>
MIME-Version: 1.0
Content-Type: multipart/alternative;
boundary="----=_NextPart_000_0000_01CB5351.46B981D0"
X-Priority: 3 (Normal)
X-Mailer: Microsoft Outlook, Build 10.0.2627
Importance: Normal

Rozdiely v hlavičke e-mailu

webmail

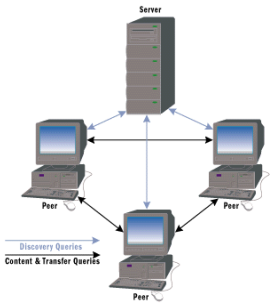
MIME-Version: 1.0
Received: by 10.100.148.11 with HTTP; Thu, 16 Sep 2010 05:52:14 -0700 (PDT)
Date: Thu, 16 Sep 2010 14:52:14 +0200
Delivered-To: radoslav.lefcik@gmail.com
Message-ID: <AANLkTin_hMoUG__DoSPi+emrL2fB6dW2FCnw0J2Yf6Gu@mail.gmail.com>
Subject:
X-Eset-AntiSpam: OK;30;calc;2010-09-16 14:52:35;1009161452350005;1840
From: a a <radoslav.lefcik@gmail.com>
To: a a <radoslav.lefcik@gmail.com>
Content-Type: text/plain; charset=ISO-8859-1
X-EsetId: 19999D284E495169069F9D7C4D1913
X-EsetScannerBuild: 7827

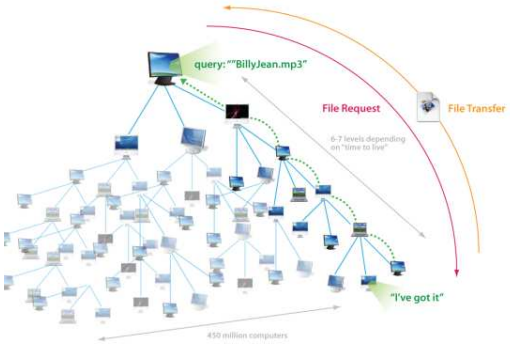
e-mailový klient

Return-Path: <radoslav.lefcik@gmail.com>
Received: from predator (static-dsl-117.213-160-175.telecom.sk [213.160.175.117])
by mx.google.com with ESMTPS id 24sm2450943bkr.7.2010.09.16.05.49.44
(version=SSLv3 cipher=RC4-MD5);
Thu, 16 Sep 2010 05:49:45 -0700 (PDT)
Message-ID: <DE5D9ADF93CB4474AE76FECF79A97A65@predator>
From: =?iso-8859-2?Q?Radoslav_Lef=E8=EDk?= <radoslav.lefcik@gmail.com>
To: <radoslav.lefcik@gmail.com>
Subject:
X-Eset-AntiSpam: OK;30;calc;2010-09-16 14:49:52;1009161449520004;A41A
Date: Thu, 16 Sep 2010 14:49:43 +0200
MIME-Version: 1.0
Content-Type: multipart/alternative;
boundary="----=_NextPart_000_001D_01CB55AE.65C7E260"
X-Priority: 3
X-MSMail-Priority: Normal
X-Mailer: Microsoft Outlook Express 6.00.2900.5931
X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2900.5994
X-EsetScannerBuild: 7827

P2P siete (Peer to Peer)

- Často používané na zdieľanie súborov,
- Hlavne na šírenie diel chránených autorským zákonom, detskej pornografie, vírusov a spamov,





Sociálne siete

- skupina ľudí, ktorej jednotliví členovia sa zoskupujú do špecifických podskupín
- nebezpečenstvo:
  - zneužívanie osobných údajov
  - zneužívanie fotografii

Napríklad:

- Facebook, MySpace, YouTube, Twitter...

Otázky?