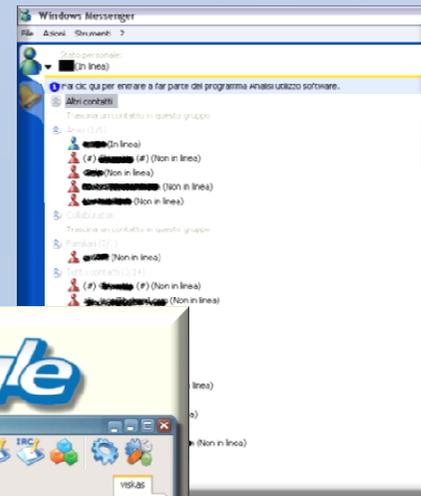


Le nuove tecnologie Rischi e rimedi



•Internet

- Chat e messaggeria istantanea
- Peer to peer
- Tv on-line

•Telefonia cellulare

- Sms – Mms
- DVB-H

- Memorie esterne

I pericoli della Rete

Navigare su Internet può essere utile e divertente, ma nella **Rete** possono nascondersi molti pericoli.

- Pedofilia,
- prostituzione,
- truffe,
- terrorismo,
- riciclaggio,
- Hacking.



la Rete ha offerto nuovi strumenti ai vecchi reati, generando
allo stesso tempo nuove forme di illegalità.

Quali sono i **reati** e i **rischi**
più comuni in Rete?

Come possiamo difenderci?

Intercettazioni	Crittografare con un programma “plug-in” in grado di eseguire il processo di codifica e decodifica del testo
Virus, trojan e worm	Antivirus che rilevi anche trojan e dialer
Hacking	Il firewall è un software che agisce come filtro
Truffe e phishing	controllare sempre che il sito dove si immettono informazioni personali
e-commerce	raccogliere il maggior numero di informazioni possibili sulla controparte contrattuale, essere a conoscenza anche dell'indirizzo e del numero di telefono, Nella UE vigono speciali normative x il diritto di recesso per la merce difettosa.
spamming	filtro anti-spam
dialer	Disabilitare tutti i numeri con prefisso 144, 166, 163, 164, 709, 899



Internet e i minori



la Rete per i bambini e i ragazzi può essere un ambiente a rischio, che offre libero accesso a contenuti di ogni genere

- chat room e siti con materiale pornografico.



Quando si parla di **pedofilia on line** ci si riferisce al comportamento di adulti pedofili che utilizzano la Rete per incontrare

- altri pedofili
- rintracciare e scambiare **materiale fotografico o video pedopornografici**
- ottenere contatti o incontri con i bambini che navigano in Rete



Un pedofilo può adescare un minore stabilendo contatti nelle

- conversazioni in chat
- nella messaggistica
- nella posta elettronica
- nelle aree di discussione dei portali



Come difendersi dalla pedofilia on line e rischi legati all'uso di internet



- È importante far capire ai più piccoli l'importanza di non rivelare in **Rete**:
 - la loro identità,
 - il numero di telefono,
 - l'indirizzo o qualunque tipo di informazione personale.



- Se il computer viene collocato in una stanza centrale della casa, anziché nella camera dei ragazzi, è più facile affiancarli nella navigazione, per capire quali sono i loro interessi e consigliarli opportunamente.



- **www.davide.it** è un esempio di portale che consente un **accesso filtrato** a Internet: collegandosi alla Rete attraverso il portale, entra in azione un filtro, che impedisce la visione dei siti contenenti pornografia, violenza e pedofilia.



• I **filtri** di navigazione sono sistemi automatizzati gestiti da software che "respingono" le pagine web dal contenuto nocivo. agiscono **bloccando** l'accesso ai siti sconsigliati presenti su una lista aggiornabile.



- Con **Internet Explorer** e **Netscape Navigator** è possibile impostare filtri che garantiscono ai più piccoli una "navigazione protetta".
- Entrambi i browser si avvalgono di un software, **RSACi**, che è collegato a una banca dati contenente una serie di siti sconsigliati ai minori.
- L'associazione internazionale che dal 1999 si occupa dello sviluppo di questo sistema è l'**ICRA** (Associazione per la valutazione di contenuti Internet).



Com'è possibile controllare la navigazione?

Il luogo di collocazione del computer connesso a Internet rappresenta un fattore di sicurezza per effettuare il monitoraggio della navigazione dei minori.


Alto rischio

La collocazione del computer nella:

- stanza del minore
- nello studio del genitore, specie in sua assenza durante le ore serali.


Basso rischio

- Le zone “di transito” dell’abitazione,
- quelle maggiormente frequentate dagli adulti
 - salone e cucina

- ➔ •I "client" di chat sono dei veri e propri programmi
- ➔ •Vanno scaricati dalla rete ed installati nel proprio PC
- ➔ •Per funzionare necessitano solo di una connessione Internet attiva e non è quindi necessario aprire il proprio browser di navigazione per chattare.
- ➔ •Attualmente hanno molto successo i programmi di Instant Messaging, cioè programmi per chattare tramite messaggi in tempo reale e non solo:
 - chat testuali con due o più utenti
 - anche chat in audio e videoconferenza,
 - scambiare files,
 - inviare e-mail
 - molto altro.

I Principali Chat Client



ICQ



AOL MESSENGER



MSN MESSENGER



WINDOWS MESSENGER



C6



YAHOO! MESSENGER



WILD



ODIGO / EVA MESSENGER / QPID



CHEETA-CHAT

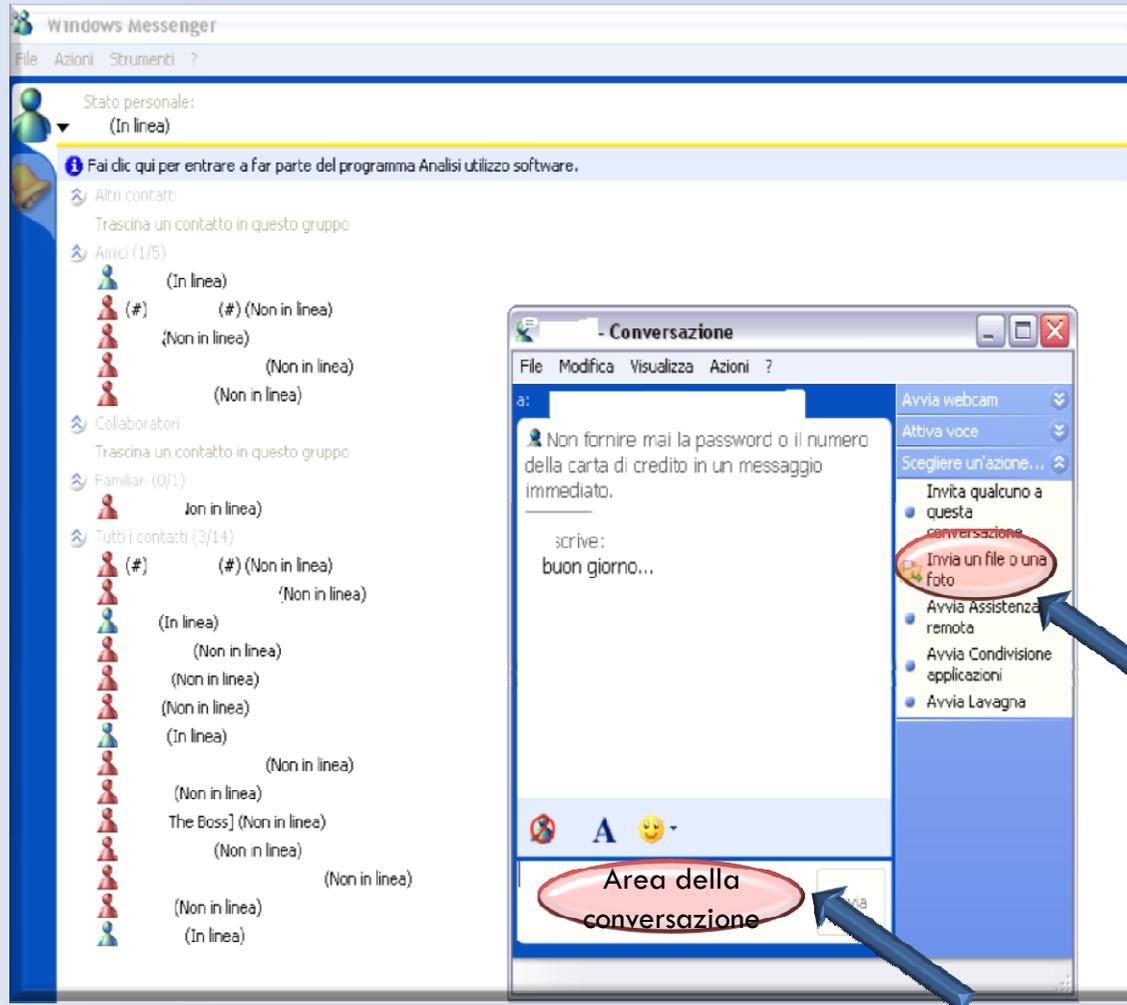


TRILLIAN



EXODUS

I sistemi di messaggia istantanea . . . Un esempio



•L'utente che effettua una connessione può:

•Scambiare messaggi istantanei

•Scambiare materiale di diversa natura:

•Audio

•Vido

•Foto e immagini

•Testi.

Peer to peer

Che cosa è il P2P ?

- Il P2P è una tecnologia che permette agli utenti Internet di poter condividere i propri file con altri.
- Internet è diventato il mezzo più usato e facile per condividere :
 - Musica
 - Film
 - Tanti altri tipi di file.

Quali sono i rischi introdotti dalla tecnologia “P2P” ?

1 - Installazione di codici malevoli

- è difficile stabilire a priori l’affidabilità della sorgente dei dati.
- Al momento del download si potrebbero scaricare dei codici malevoli del tipo:

- Virus
- Trojan
- spyware etc.

2 - Esposizione di informazioni sensibili o personali

- usando le applicazioni P2P, si concede la possibilità ad altri utenti di avere accesso al proprio computer.
- Malintenzionati potrebbero accedere ai dati personali senza il dovuto consenso.



XMute

3- Riduzione/Negazione del servizio

- l'attività di File Sharing incrementa
 - la mole di traffico scambiato
 - il carico di lavoro del computer.

Rischio :

- Rallentamenti di ogni attività
- Rallentamento della navigazione Internet;



BitTyrant

4 - Predisposizione agli attacchi

- le applicazioni P2P richiedono di aprire nuove porte al sistema operativo o al firewall per poter scambiare dati.
- Il computer si trova ad essere maggiormente esposto ad attacchi da parte di male intenzionati.

5 - Altro

• i file disponibili sulle reti P2P possono includere:

- software piratato,
- materiale provvisto di copyright
- materiale pornografico/pedofilo.

• **Il download anche inconsapevole espone al rischio di :**

- multe o azioni legali.
- Nel caso in cui il computer faccia parte della rete di una società, sia l'utente e sia la società potrebbero essere ritenuti responsabili.



!! Attenzione ai reati !!



I Principali sistemi P2P



Gnutella1-2/Shareaza



Direct Connect



bitTorrent



Kazaa/FastTrack



ed2k/eMule



Manolito/Blubster

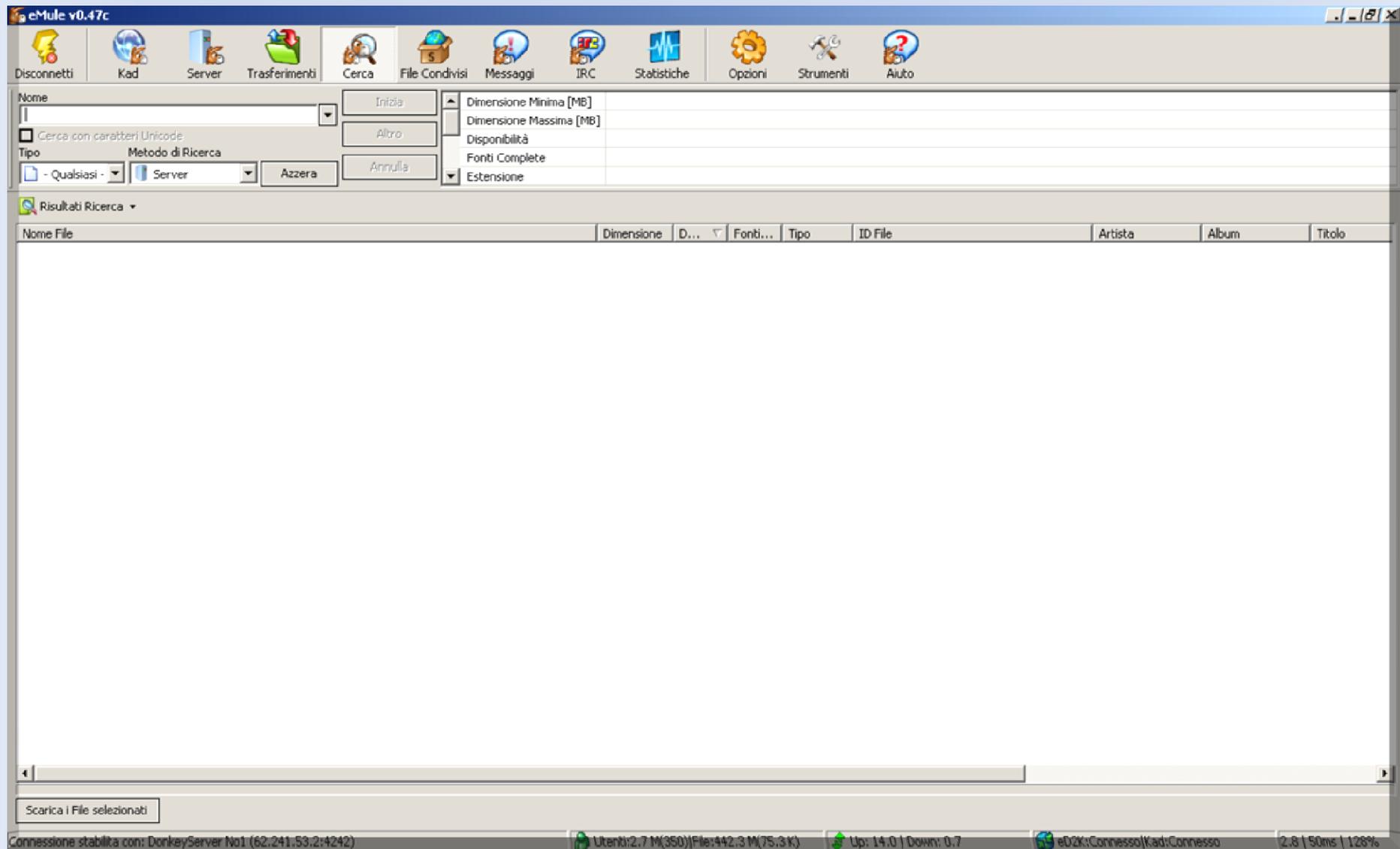


OpenNap clients



Altri client

Un Esempio: Emule



Si possono limitare i rischi ?

N.B. Il miglior consiglio, in assoluto, sarebbe quello di evitare di usare le applicazioni P2P.

•Mantenere aggiornato l'Antivirus

- i programmi antivirus riconoscono e proteggono il computer dalla maggior parte dei virus conosciuti.
- Il problema risiede nel fatto che giorno per giorno compaiono nuovi tipi versioni di virus; per questo è di vitale importanza mantenere aggiornato il proprio programma antivirus;

•Usare un Personal Firewall

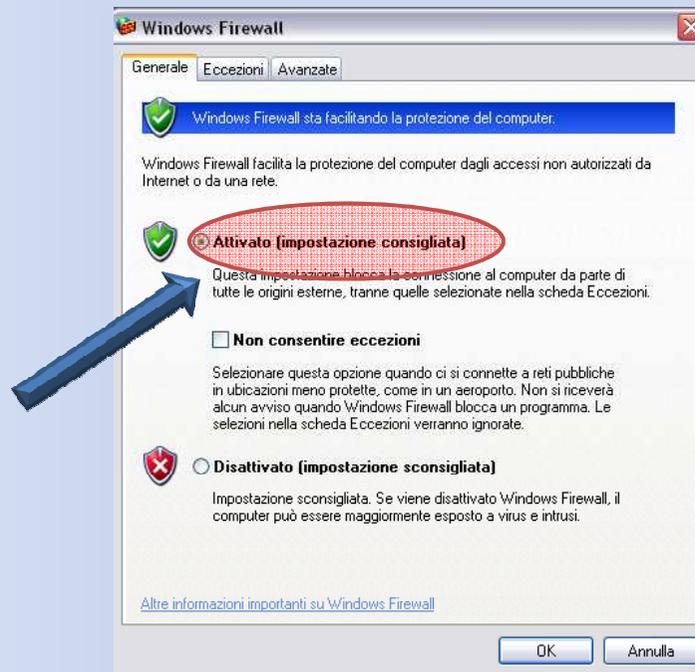
- un buon Personal Firewall potrà aiutare a tenere sotto controllo il traffico in uscita ed in entrata.

Il Firewall personale

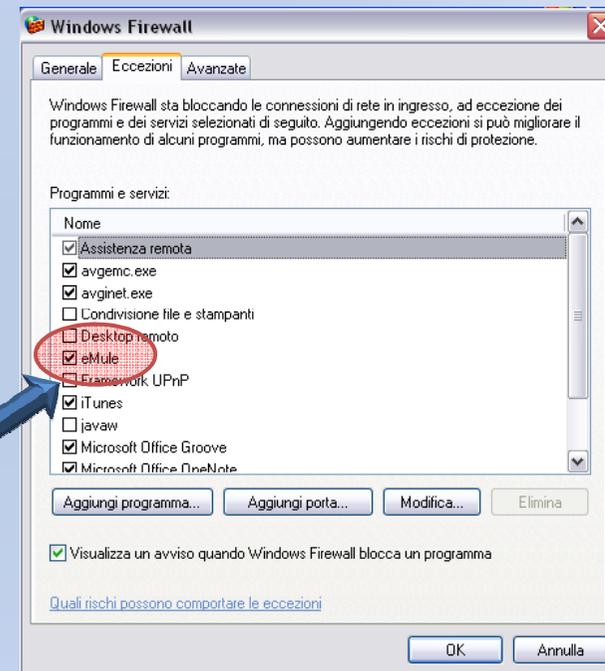
Utilizzare un Firewall, consente di prevenire intrusioni
E protegge da connessioni a server P2P



L'importanza di verificare le impostazioni del Firewall personale



Attivando il personal Firewall
L'utente può tutelare i propri dati
E impedire che applicativi potenzialmente
Pericolosi si connettano ad Internet,
Causando problemi.



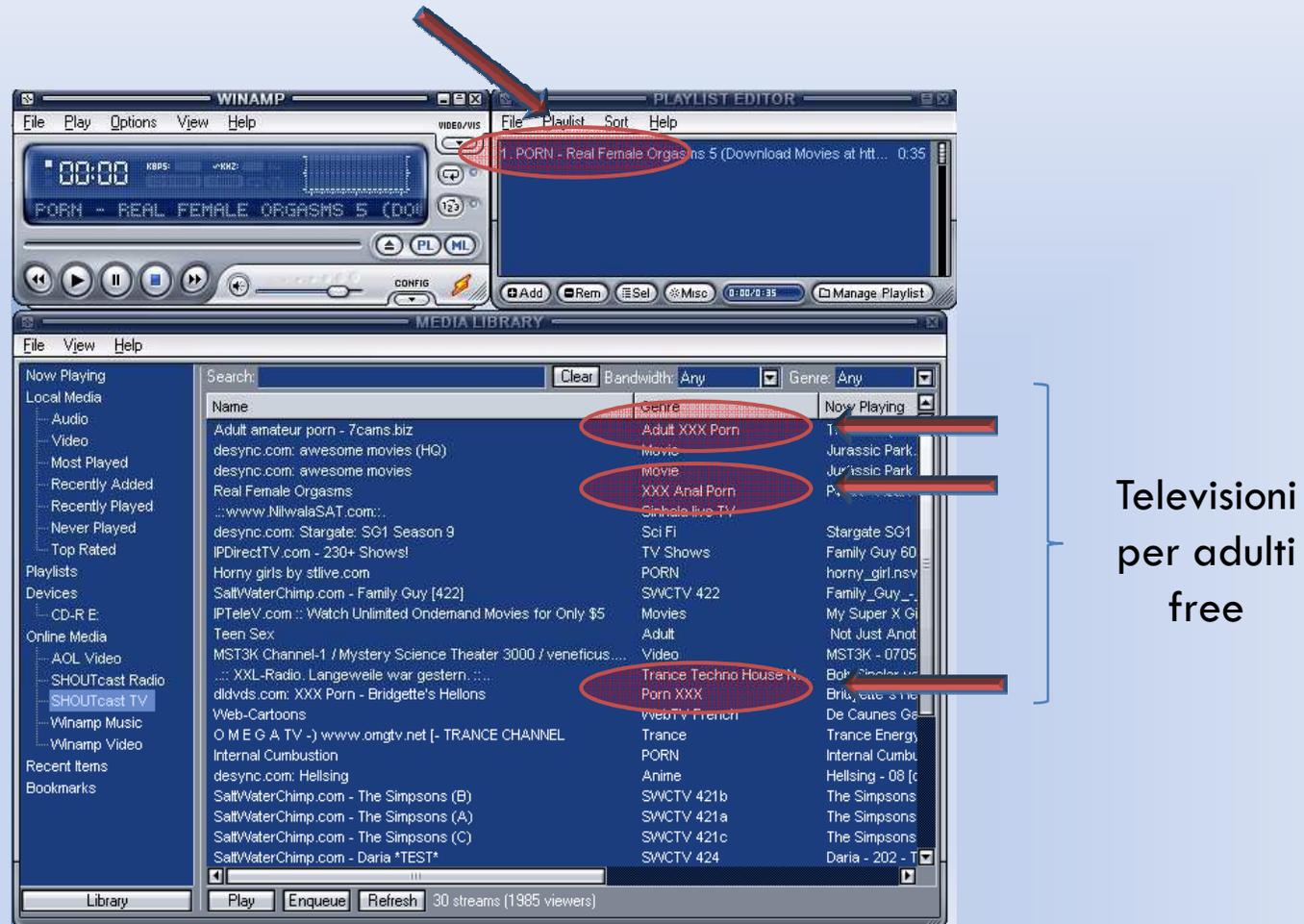
Applicativi del tipo P2P si "aprono" una porta
Nel firewall, consentendo ad altri utenti
Di sbirciare nei file del nostro PC

Televisioni via internet – un esempio



Le televisioni digitali ON-Line possono essere viste grazie ai più comuni software di intrattenimento musicale quali:

- Windows Media Player
- Winamp



Anche gli applicativi “ricreativi” come i più comuni lettori Mp3 possono nascondere dei dati sensibili e di natura pornografica, è quindi opportuno monitorare con attenzione anche questi programmi.

Cellulari e Videofonini

La telefonia portatile ha negli anni avuto una forte espansione
le potenzialità dei telefoni portatili oggi sono innumerevoli e
ad alto rischio.

la sempre maggior diffusione di apparati complessi e molto
Perfomanti merita una certa attenzione



L'evoluzione della telefonia cellulare – le generazioni

1°
generazione

E-Tacs

- Sistema di telefonia mobile analogico.
- Sbarca in Italia nel 1990 e subito ha un successo tale da saturare il traffico mobile.
- E' stata decisa la dismissione della rete E-Tacs nel 2007.



2°
generazione

GSM

- Global System for Mobile Communications
- Standard internazionale per la telefonia cellulare digitale.



3°
generazione

UMTS

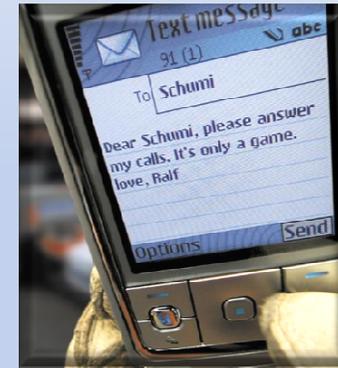
- Universal Mobile Telecommunications System
- Sistema mobile sviluppato dai maggiori operatori mondiali nell'ambito del progetto IMT-2000, basato sull'architettura GSM.



Cellulari e Videofonini – MMS, SMS

MMS – Multimedia Messaging Service - Servizio di messagistica multimediale che consente la creazione di messaggi contenenti una combinazione di:

- testo,
- immagini,
- suoni,
- melodie,
- filmati. Possono essere spediti ad un qualunque cellulare compatibile.



SMS - Short Message Service - Servizio messaggi brevi –

- permette di inviare o ricevere messaggi di 160 caratteri o più.
- Tramite gli SMS possono essere spediti loghi e suonerie.
- Gli SMS sono uno dei maggiori successi commerciali del GSM, il loro utilizzo ormai è diventato parte della vita quotidiana
- in alcuni paesi è stato creato un nuovo linguaggio appositamente utilizzato per gli SMS.

Cellulari e Videofonini – Fotografia e video

Le fotocamere dei cellulari di ultima generazione sono diventate vere e proprie macchine fotografiche digitali, con la doppia funzionalità:

- fotocamera digitale
- Videocamere digitale

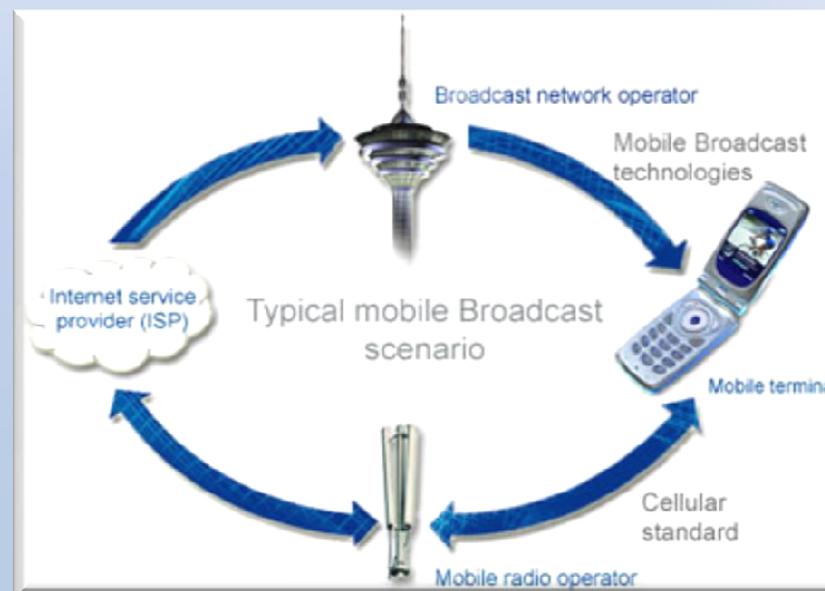


Le fotografie e i filmati prodotti con tali apparati, sono qualitativamente pregievoli e facilmente trasmettibili ad altri apparecchi.

La Tv sul cellulare

DVB-H

- Acronimo di Digital Video Broadcast - Handheld.
- standard per la trasmissione di contenuti televisivi in forma digitale su dispositivi portatili compatibili come telefonini e palmari



In Italia il servizio è oramai pienamente operativo è la tipologia dei programmi che si possono vedere sono i più svariati, compresi canali pornografici.

Le schede SIM dei telefonini vanno limitate chiedendo al proprio gestore di impedire la visione di tali canali.

Cellulari e Videofonini – Come trasferire dati tra diversi apparati

IrDA

- Infrared Data Association
- Le 'porte IrDA' presenti su numerosi telefoni cellulari, computer portatili e palmari consentono l'interscambio di informazioni senza l'utilizzo di cavi di collegamento, in modo pratico ed economico.



Bluetooth

- Sistema di trasmissione dei dati fra cellulari o dispositivi portatili che utilizza le onde radio invece degli infrarossi come l' IrDA.
- Prende il nome in onore del re vichingo Harald Bluetooth, che unì Danimarca e Norvegia.

Cavi Seriali o USB

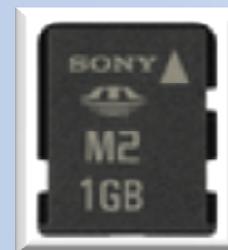
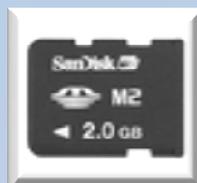
- I cavi in dotazione con i telefoni cellulari consentono di interfacciare l'apparato mobile con un PC in modo da travasarne e sincronizzarne il contenuto
- spesso necessitano di specifiche Suite applicative fornite dal produttore che facilitano il riconoscimento dell'apparato e la gestione delle risorse



Mobile Divece Memory

In commercio è possibile trovare una vasta
Gamma di espansione di memoria per i telefoni
Di ultima generazione, in grado di contenere
Dati multimediali quali:

- Video
- Audio
- Fotografie

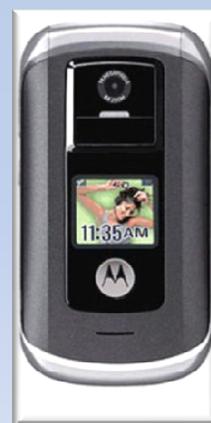
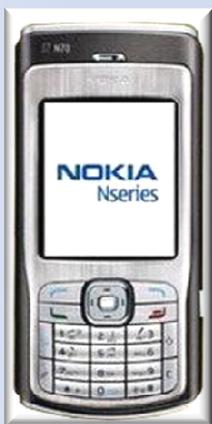


Multi-card reader

Le memorie esterne per telefoni cellulari possono
Essere agevolmente ispezionate tramite l'utilizzo
Di periferiche USB da utilizzare con un PC
Sono i lettori multi-schede.
Strumenti molto utili ed estremamente economici



Cellulari e Videofonini – Alcuni esempi



Videofonino
Ultima
generazione

Cellulare "base"