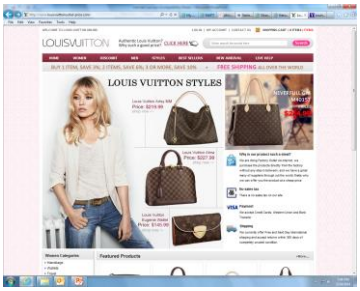
Training Manual on IP Crime Prosecution

10. IP Crime on the Internet

Internet

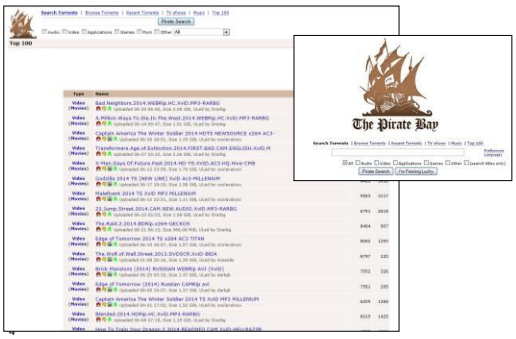
- Network of computers connected by wire or wireless means
- Communicating via software systems or “protocols”
- Users gain access via Internet Service Providers
- Each Internet connection is given an IP (**I**nternet **P**rotocol) number by ISP

Thousands of web sites selling fakes



3

Web sites gather links to infringing copies

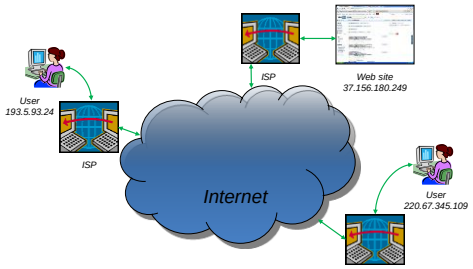


4

Other web sites “stream” content without copying – especially live sports

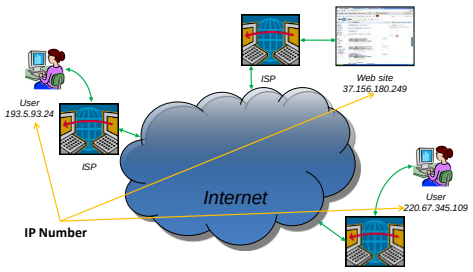
5

Users and web sites



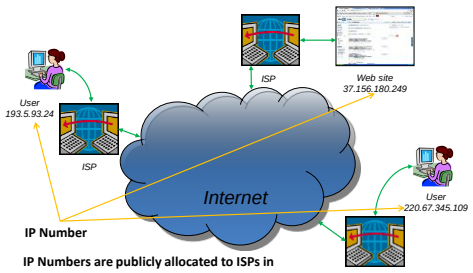
6

Users and web sites



7

Users and web sites



IP Numbers are publicly allocated to ISPs in blocks, so it is simple to find out which ISP gave access to a user at a certain IP address.

8

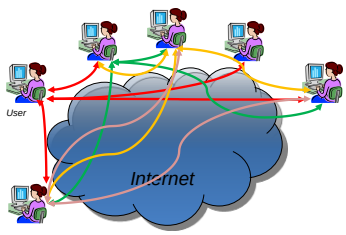
Web sites

- Web sites are identified by "Uniform Resource Locators" (URLs) - e.g., www.wipo.int
- Domain name servers list IP addresses of the web sites identified by such URLs. The domain name server converts the URL into an IP address and directs the user's internet browser to that address.
- ISPs can hinder access to specific URLs or IP addresses through web site blocking

Crime and Internet

- Internet + digitisation of entertainment products
  = massive online copyright piracy
- Cheap global reach via WWW + problems of cross-border enforcement + efficient global trade & postal services
  = massive importation of counterfeits

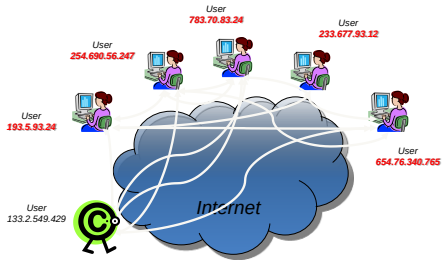
Peer-to-Peer systems allow many users to "share" (copy) content



Receive and share slices of content

11

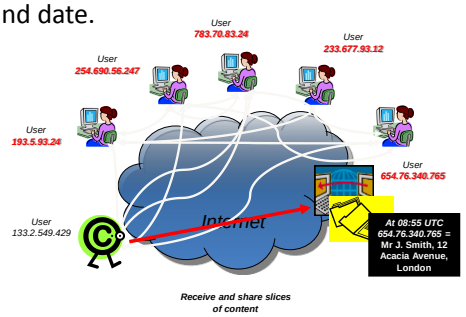
Investigator can participate in network to collect IP numbers of infringers



Receive and share slices of content

12

Then require ISP to check which subscriber had a certain IP number at a certain time and date.



Trademarks and Internet

- Typically counterfeiting concerns physical goods – the use of the mark may be on the goods or the web site. But service marks can be infringed too.
- If there is a sale to a purchaser in the jurisdiction, infringing use of the mark takes place at least there.
- If offers to sell are targeted at the jurisdiction, infringing use of the mark takes place there.
- Evidence of targeting: language, currency, prior dealings, country domain (e.g.: fakes.co.**uk**).

Copyright and Internet

- Copyright works, films, sound recordings and broadcasts are protected in the digital environment as in the offline world.
- Subject to limited exceptions for quotation etc, right holder can prevent copying and communication to the public of his work.
- When A 'sends' a work to B, a copy is made on B's computer.
- Making a work available online without permission results in an infringing communication to the public.
- A communication targeted at the jurisdiction results in an act within the jurisdiction, irrespective of location of the defendant.
- Criminal liability may depend on 'commercial scale'.

ISP liability: 'safe harbors'

- Under statute, an exemption from liability is usually given to:
  - *An ISP, in relation to copies made during the neutral, technical process of giving internet access to subscribers*
  - *A web site passively hosting content uploaded by others.*
- However, they must satisfy specific conditions, to establish that they are not actively involved in the infringement.
- The liability for infringement of the person primarily responsible remains unaffected.
- ISPs remain subject to duty to assist the public authorities when legally required to do so by a warrant or otherwise.

Crime and Internet

- Criminal procedure may permit the prosecutor to seize the domain name of infringing web site.
- Money-laundering powers useful to freeze assets.
- Delocalization and anonymity help the criminal, but difficult to act on the Internet without leaving traces.
- Investigation requires special skills – online IP crime is a subset of cybercrime.
- Traditional skills of the detective remain important.