## Lars Underbjerg

My name is Lars Underbjerg and I'm Danish police officer working at the National High Tech Crime Centre since more than 10 years. I'm investigating online child abuse cases involving forensic examination of computers, victim and offender identification, public complaints, international cases, classification of child abuse material, evaluation of websites for the Danish filter list and all other matters related to online child abuse cases. Since 2001 I have been a member of Interpol's Expert Group on Crimes against Children. Since 2004 I have been a member of CIRCAMP (COSPOL Internet Related Child Abusive Material Project) that in the last couple of years has been dealing with the law enforcement angel into filtering websites containing child abuse material. CIRCAMP has just finished a 2 year project funded by the Safer Internet program under the European Commission.
http://www.circamp.eu

## Background for filtering child abuse websites in Denmark

Following Norway and Sweden who started filtering child abuse websites in 2004 and 2005 Danish ISP's (Internet Service Provider) started filtering child abuse websites in October 2005. Before that it had been agreed that Danish National Police should evaluate suspected websites and create the filter list for the ISP's. From the start all major ISP's joined the project. Those ISP's covered about 95% of the private Internet customers. From the beginning there was a clear definition of responsibilities between ISP's and Danish National Police in written agreements. Danish National Police evaluates the material according to Danish Criminal Law and provides a filter list to involved ISP's. The involved ISP's then filter websites on their own network according to their own policy. No law has been implemented.

## General information

Before receiving the filter list from Danish National Police an ISP must sign a written agreement defining the responsibility of each party.

Danish National Police receives information on child abuse websites and evaluate each websites before adding or excluding it to the filter list. The filter list contains domains and sub domains that can be filtered by changing records on the DNS servers (translates IP numbers and domain names) of the ISP. Danish National Police receives information on child abuse websites from ISP's, public complaints, forensic examinations of computers, NGO hotlines and international law enforcement cooperation.

At team of not more than 4 specially assigned police officers is evaluating each reported domain/sub domain according to Danish Criminal Law. If a domain/sub domain goes into the filter list the illegal content is documented and stored in an archive. Only domains containing explicit

child abuse material are added to the list. Groups, image sharing communities and such are not added to the list but the content is reported to the owner of these services. Information on filtered domains is shared among the international law enforcement cooperation.
The filter list is updated daily since websites containing child abuse material is very dynamic. Many of those websites only exists in a short period and change server location on a daily basis to avoid being investigated by police and to avoid filtering.
Only domains that have been requested by a customer within the last 3 months are in the filter list. The actual Danish filter list affects 364 domains.

The filter list is stored on a secure server at the Danish National Police. Each involved ISP is every night fetching the daily updated filter list from the secure police server and implementing the list on their DNS servers. Only designated personnel is handling the filter list at ISP level.

When a customer of an ISP requests a domain which is included in the filter list that customer is redirected to a STOP page informing that the website requested has been filtered on the basis of child abuse material. Information on where to complain about the filtering is listed on the STOP page.
Since 2005 less than 10 complaints related to filtering have been reported to Danish National Police. When a complaint is received Danish National Police look into the archive to explain why the domain was filtered initially. An online check is also done and if the domain at the time for the complaint does not contain child abuse material that domain is removed from the filter list. There have been no economical claims against a domain being filtered due to child abuse material.

Through Europol's websites the owner of commercial websites are able to get information on in which countries they are blocked. If they are filtered they are referred to the national agency that is in charge for the filtering to get more information.

Domains registered, managed or hosted in relation to Denmark are not filtered but investigated in traditional way to be able to identify those who take part in distribution of child abuse material.

Due to the fact that illegal domains changes location and providers in a very dynamic way it has very little effect to report filtering of a domain to an ISP outside Danish jurisdiction. It also only has effect to report a filtered domain to another law enforcement agency if that agency follows up on your requests and are able to cooperate with the involved ISP. Suggestion by opponents of filtering has been made that the owner of a domain should be notified when the domain is added to a filter list. That would be the same as informing a suspects that he is under investigation.

The suggested ”take down strategy” only works in the ideal world, not in the practical daily work. Many countries do not have this as a priority or there is a lack of cooperation from the involved ISP. Many domains only exist in a few days and many countries do not have legislation in place to secure evidence before taking domains down. In that way evidence is lost. Denmark is only informing close law enforcement partners when a domain in their country is added to the Danish filter list to ensure to most efficient police investigation.

Filtering works even if domains changes location due to the DNS system. The domain name will just be redirected to another IP.
If a domain is “taken down” it will most likely appear at another location shortly after and police have to initiate a ”take down” again together with all other law enforcement agencies in the world. Instead of having law enforcement agencies all over the world chase the same domains round the world filtering domains on a national level is an option.

At Interpol a “worst of” list created in cooperation between CIRCAMP and Interpol is distributed to countries where no law enforcement agency is maintaining a national filter list. This list contains domains with the “worst of” child abuse material. The criteria’s is that it must depict a child below the age of 13 years involved in explicit sexual activity. For a specific day in November the “worst of” list affected 246 domains. The “worst of” list is maintained by a designated officer at Interpol and is updated almost on a daily basis.
16 days after the creation of that specific “worst of” list I resolved 168 of the 246 domains. That means that I was able to access 168 of the domains that were on the list 16 days before. The difference of 78 domains shows how dynamic the existence of these websites is. For those domains of the 168 I was able to lookup (country locate), they were located as follows:

CA 4, CN 5, CZ 2, DE 1, GB 5, JP 2, KR 4, NL 5, RU 10, SE 2, US 126

These figures are based on time of the lookup and not the time when they were added to the list. The country location can have changed during the 16 days.

Reporting 126 domains to US and 10 to RU for a “take down” would have little or no effect since it has low or no priority in these countries.
Therefore filtering these domains have the effect that Danish end users will not be exposed to child abuse material distributed from these domains. From a law enforcement perspective this is positive and taking part in the preventive policing of the Internet. Since Denmark started filtering child abuse websites less websites has been reported by the public to the police hotline.

This year there have been a decrease in the number customers filtered in Denmark. The procedures on how long time a domain was in the Danish filter list was changed and this lead to this decrease. From 2005 to 2009 roughly between 2500 and 3000 different computers were filtered per day.

In Denmark there are no statistics on the percentage of commercial websites filtered.

Denmark has developed and implemented software and procedures so that 1 police officer within 1 hour per day can do all work related to maintaining the filter list.