



## USB Threat Evaluation - Detection and Reporting System

### Content Removal Trace Report

Date Range: 28-Apr-2007 - 28-Apr-2007

Group: NextSysSecure, Inc

Run Date: April 28, 2007

User Name	System Name	Network Address	Removal Date	Filename
AICapone	COMPUTER2	192.168.0.100	2007-04-28 11:41:35	Source->C://Documents and Settings//AICapone//My Documents//Customer List.xls,, USB -->H://Customer List.xls
AICapone	COMPUTER2	192.168.0.100	2007-04-28 11:41:42	Source->H://Customer List.xls,, USB --> H://Copy of Customer List.xls

Total Content Removal for "AICapone" = 2

User Name	System Name	Network Address	Removal Date	Filename
Guest	COMPUTER1	192.168.0.151	2007-04-28 13:07:03	Source->C://Documents and Settings//Guest//My Documents//Sales Presentation.ppt,, USB -->H://Sales Presentation.ppt

Total Content Removal for "Guest" = 1

User Name	System Name	Network Address	Removal Date	Filename
Tom Jones	COMPUTER4	192.168.0.155	2007-04-28 10:02:13	Source->C://Documents and Settings//Tom Jones//My Documents//Network Settings.doc,, USB --> F://Network Settings.doc
Tom Jones	COMPUTER4	192.168.0.155	2007-04-28 10:03:40	Source->C://Documents and Settings//Tom Jones//My Documents//Network.dwg,, USB -->F://Network.dwg
Tom Jones	COMPUTER4	192.168.0.155	2007-04-28 15:25:54	Source->C://Documents and Settings//Tom Jones//My Documents//Emergency Action.doc,, USB -->F://Emergency Action.doc
Tom Jones	COMPUTER4	192.168.0.155	2007-04-28 17:15:11	Source->C://Documents and Settings//Tom Jones//My Documents//Facilities.dwg,, USB -->F://Facilities.dwg

Total Content Removal for "Tom Jones" = 4

**Content Removal Trace Report provides the security administrator with a list of corporate Files removed by each employee. Each time a file is copied to a portable USB mass storage device, USBmon creates a real time log file entry and a database record capturing the file name removed, user id, computer name, network address and USB device serial number it was copied to. The report provides the security administrator with forensic type list of all files removed and identifies who did the removal**