Ethical Hacking and Countermeasures

Version 6

Module XLVI

Securing Laptop Computers

InformationWeek
BUSINESS INNOVATION POWERED BY TECHNOLOGY

Laptop Stolen With Personal Data On 300,000 Health Insurance Clients

Horizon Blue Cross Blue Shield of New Jersey is offering its members free credit monitoring for one year as a result of the security breach.

By Marianne Kolbasuk McGee, InformationWeek
Jan. 30, 2008
URL: http://www.informationweek.com/story/showArticle.jhtml?articleID=206100526

Horizon Blue Cross Blue Shield of New Jersey has notified its members that an employee laptop computer containing personal information -- including Social Security numbers -- for about 300,000 individuals was stolen in early January.

The health care insurer has sent letters to thousands of its members alerting them about the theft, which occurred in Newark, N.J., on Jan. 5. On its Web site, the company says a "security feature was initiated" on Jan. 28 that "destroys all the data on the stolen computer."

Horizon Blue Cross Blue Shield of New Jersey says the personal information contained on the computer also included names and addresses of members, but no medical data.

The company says it "believes" it is "highly unlikely" that any personal data stored on the stolen computer has been accessed and that the computer was "password protected."

Nonetheless, the insurer is offering affected members free credit monitoring for one year.

Horizon Blue Cross Blue Shield of New Jersey is the latest company to report a security breach related to a stolen laptop.

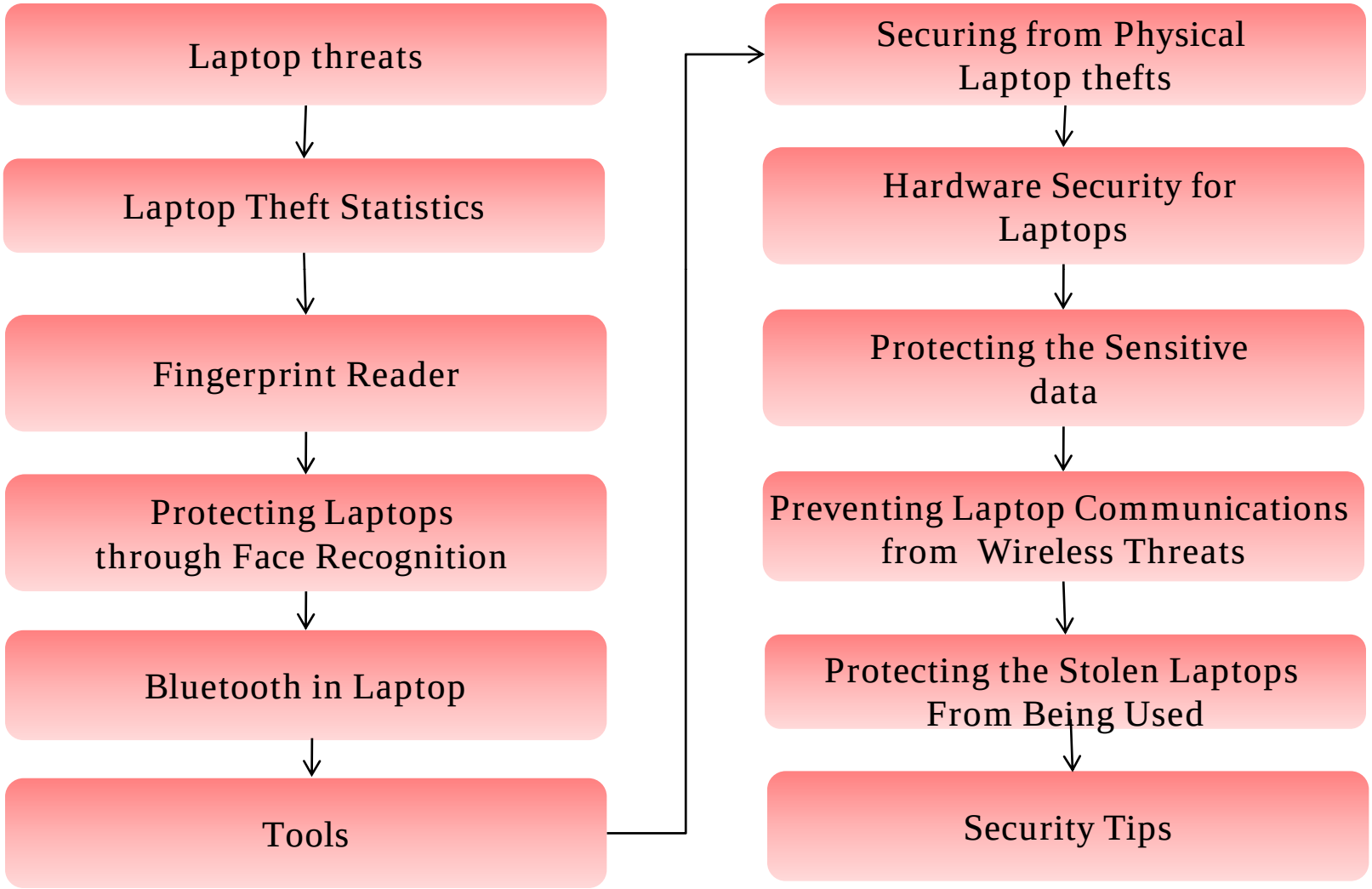
Source: *http://www.informationweek.com/*

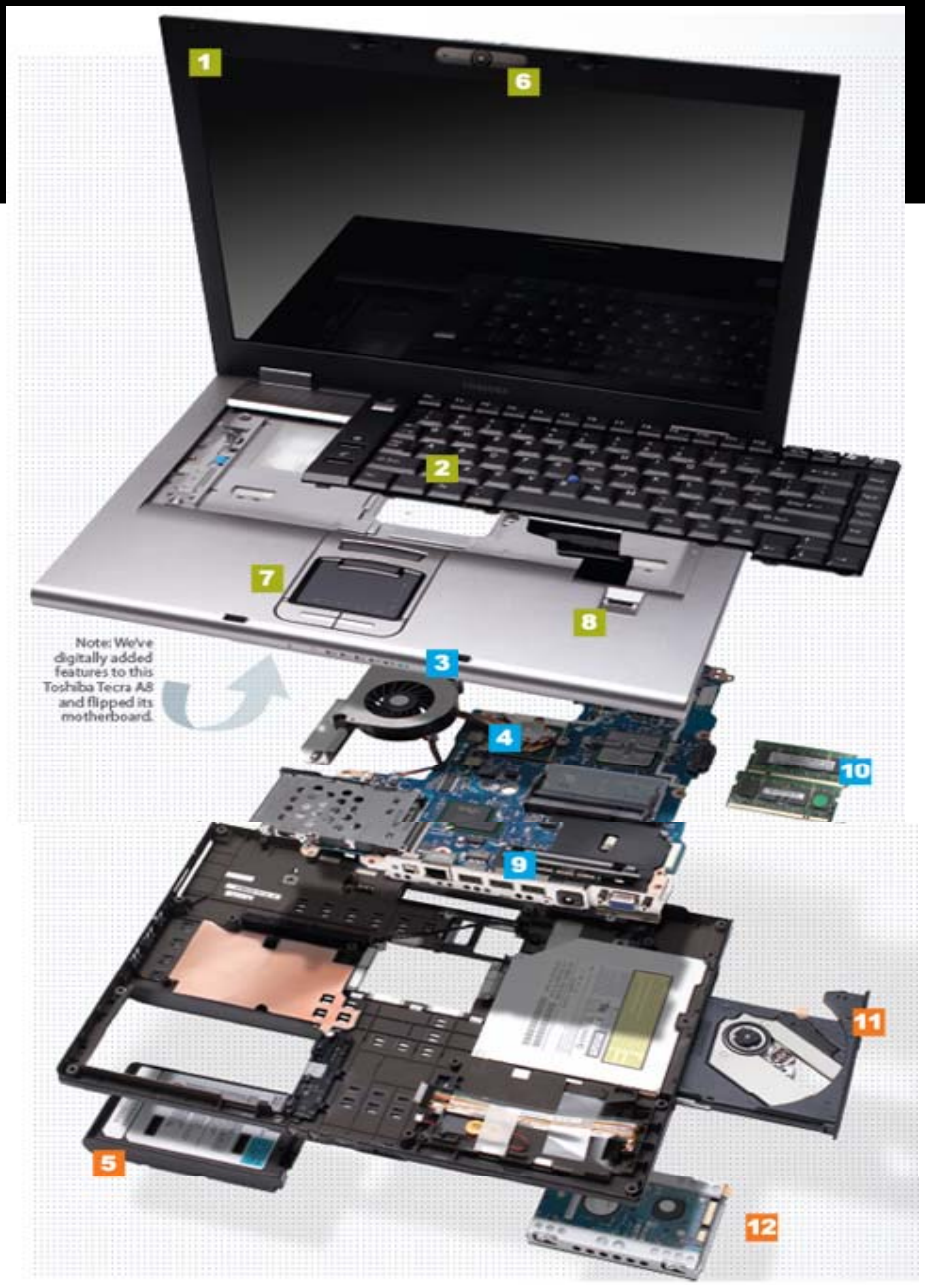
Module Objective

This module will familiarize you with:

- Laptop threats
- Laptop Theft Statistics
- Fingerprint Reader
- Protecting Laptops through Face Recognition
- Bluetooth in Laptops
- Tools
- Securing from Physical Laptop thefts
- Hardware Security for Laptops
- Protecting the Sensitive data
- Preventing Laptop Communications from Wireless Threats
- Protecting the Stolen Laptops From Being Used
- Security Tips

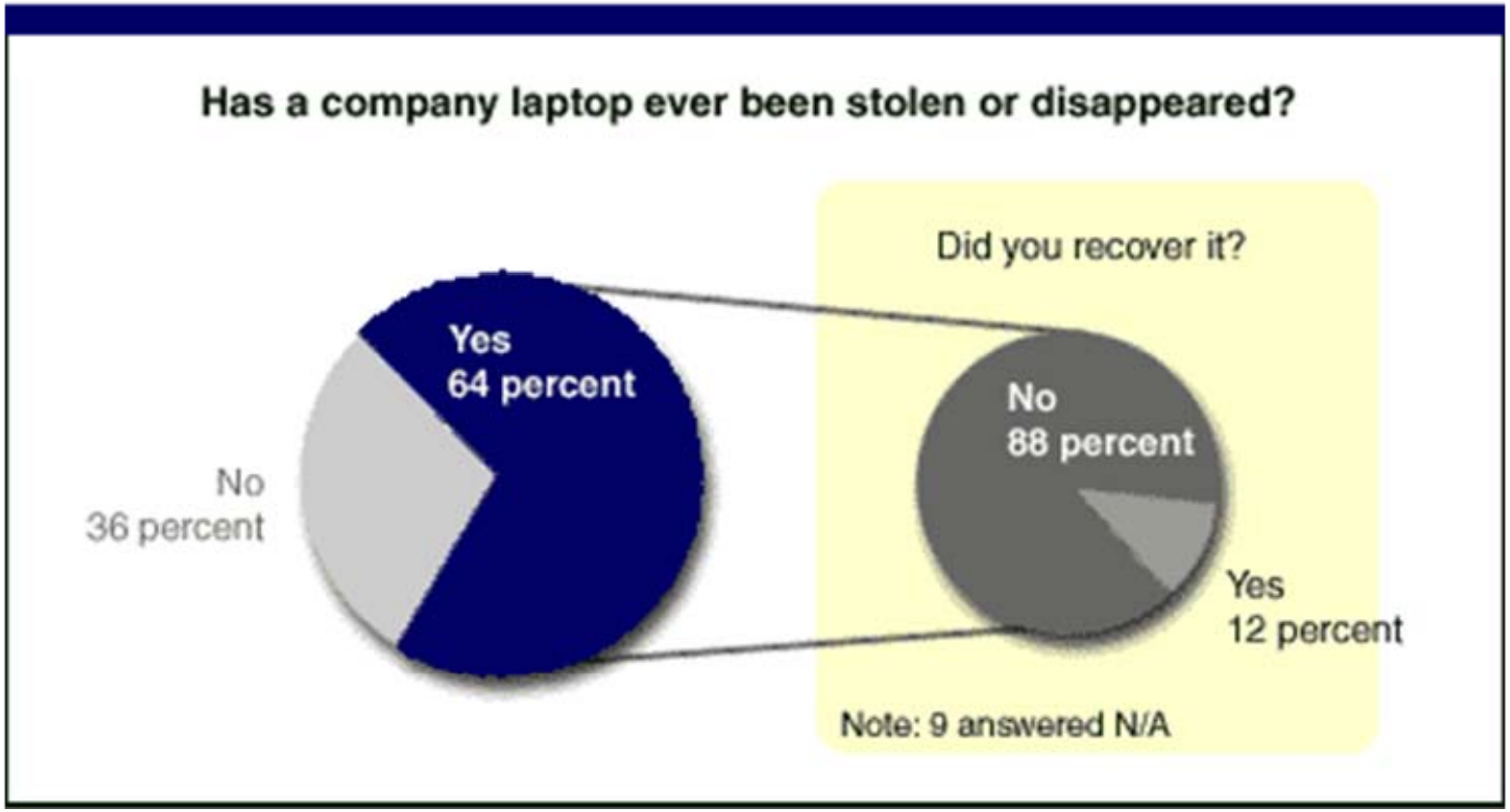
Module Flow





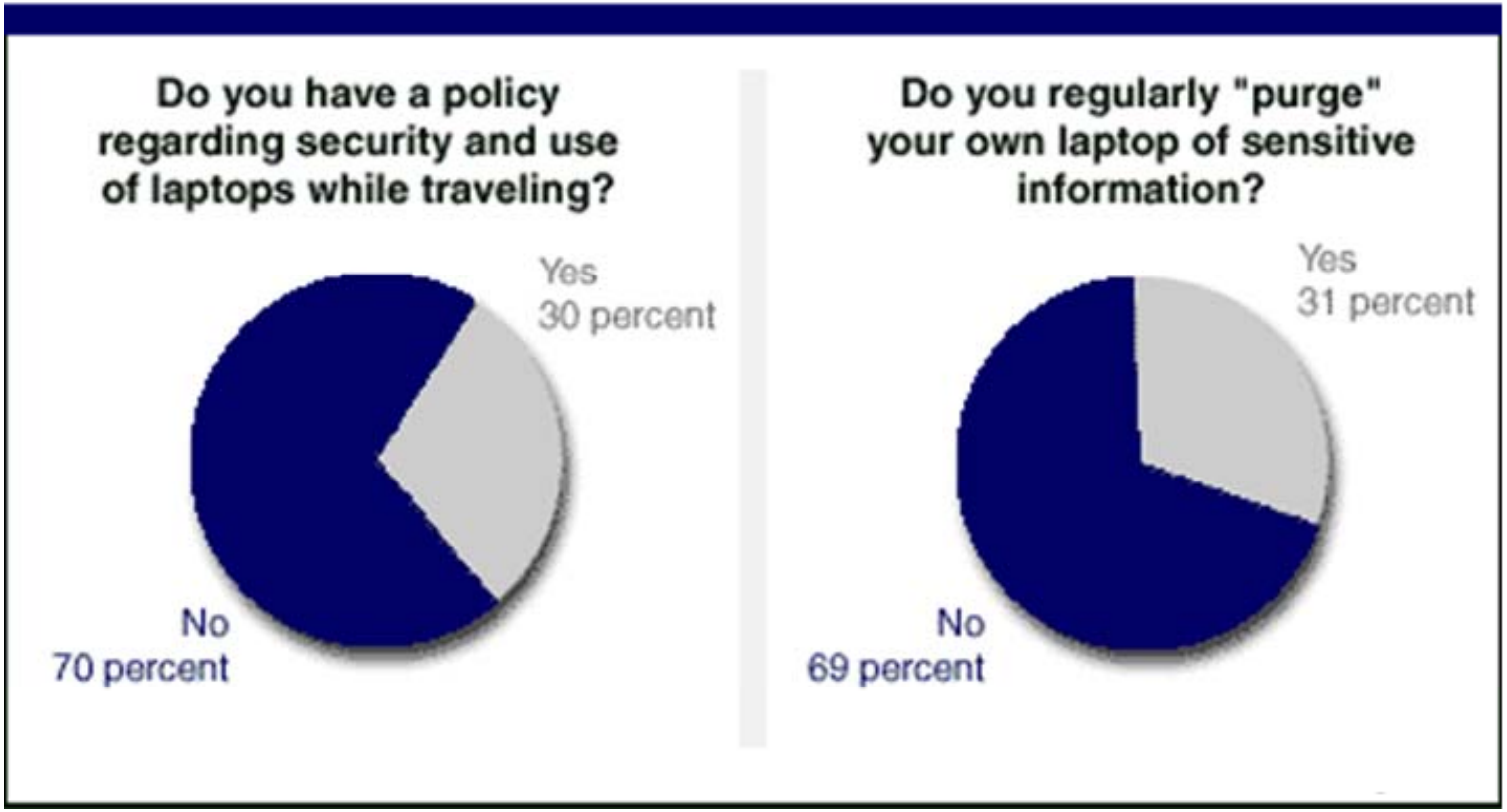
Source: *http://www.popularmechanics.com/*

Statistics for Stolen and Recovered Laptops



Source: *http://articles.techrepublic.com.com/*

Statistics on Security



Source: *http://articles.techrepublic.com.com/*

Percentage of Organizations Following the Security Measures

	Number of Organizations	Percentage of Organizations
Passwords	35	97
Encryption of data	20	56
Employee certification/signoff	20	56
Awareness training	16	44
Locking cables	13	36
Data restriction on laptop	13	36
Automatic encryption of data	12	33
Internet tracking/locator software	9	25
Smart cards	7	19
Key cards	7	19
Deletion programs	4	11
Biometric access controls	4	11
Kensington locks	2	6
Motion sensors and alarms	1	3
Travel prohibitions	1	3
Unknown	1	3
Others	0	0

Source: *http://www.iacis.org/*

Laptop Threats

Physical Security

- Criminals target laptops for quick profits and misuse of the confidential data
- Laptops containing personal and corporate information can be hacked by the attackers and used for their profits

Information Security

- Corrupting, destroying, or gaining access to a Laptop through hacking, malicious programs, or social engineering
- Accessing the data through weak passwords and open access
- Application security and vulnerabilities to attack the vulnerable application
- Attacking the laptops with unencrypted data and unprotected file systems
- Copying the data through removable drives, storage mediums, and unnecessary ports which are not disabled

Laptop Threats (cont'd)

Wireless Security

- Intercepting and monitoring wireless traffic through various sniffer tools and interception software
- Packet insertion and hijacking attacks into the sniffed wireless traffic
- Jamming is used where the attacker uses different wireless devices at different frequencies which creates radio frequency interferences for any wireless network in vicinity
- Peer to peer attacks is performed by using Ad Hoc mode
- Man in the middle attack
- Wi-phishing is used by hijackers to setup an access point with SSID that is used by default on most access points

Laptop Theft

If a laptop were lost...

- What information of a strategic nature would be disclosed? Real examples of this type of information include pending mergers, new product intellectual property, strategies and launch plans, and previously undisclosed financial operating results
- What information of a tactical nature would be disclosed? Examples include private compensation information, plans for organizational changes, proposals to clients, and the myriad of similar information that can be gained from reading a person's email, calendar, contacts, or collection of documents and spreadsheets

Laptop Theft (cont'd)

If a laptop were lost...

- What information about the company's network or computing infrastructure would be revealed that would facilitate an electronic attack?
  Examples of this type of information include usernames and passwords, dial in numbers, IP addressing schemes, DNS naming conventions, ISPs used, primary mail servers, and other networking details related to connecting the laptop to the corporate or Internet environment.
- What personal information about the laptop owner can be obtained?

Fingerprint Reader

Fingerprint Reader enables the user to access the laptop in a more secured and easy way

It provides higher level of security while accessing the data or network

BioNet 2 laptop fingerprint reader designed from Biometric fingerprint reader is specially used for portable storage devices such as laptops and PDAs

It offers secured access to the applications like, valuable logons, web links, documents, image files, and more

Protecting Laptops Through Face Recognition

Face Recognition technology is used to access authentication on the laptop by recognizing the face as the password

It takes the snapshot of the user and creates digital shots which serve as the password

It supports multiple users to allow trusted ones to access the laptop

Features:

- Advanced Face recognition software via Integrated Camera for authenticating user
- One-key recovery helps to recover operating system in case of system crash or system effected by virus

Bluetooth in Laptops

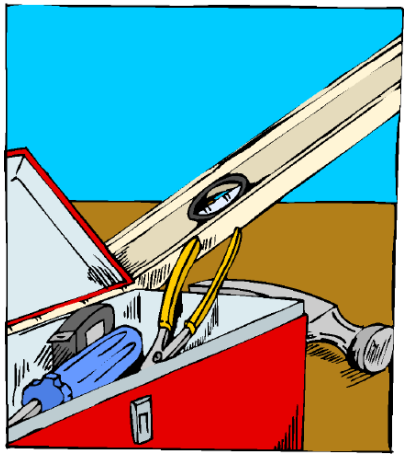
Bluetooth enables two laptop devices to connect with each other negating the usage of cables and wires

A Bluetooth enabled laptop tries to pair with another intended laptop but not with an unknown device

The Bluetooth laptop devices create an initialization key PIN code or passkey used for authentication

Attacker can sniff this session to access the data

The information passed between the two laptop devices should be encrypted which is upto 128 bits



Tools

Laptop Security

Laptops can be secured physically from being stolen or lost by using security tools

The tools will let the laptop to be fixed at one place, lock it to an immovable device or use secured laptop trolleys

Laptop Security Tools

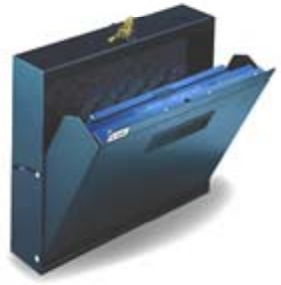
Steel Cable Locks

Laptop Tie-down Brackets

LapSafe laptop trolley

Portable Laptop Carts

Laptop Locker



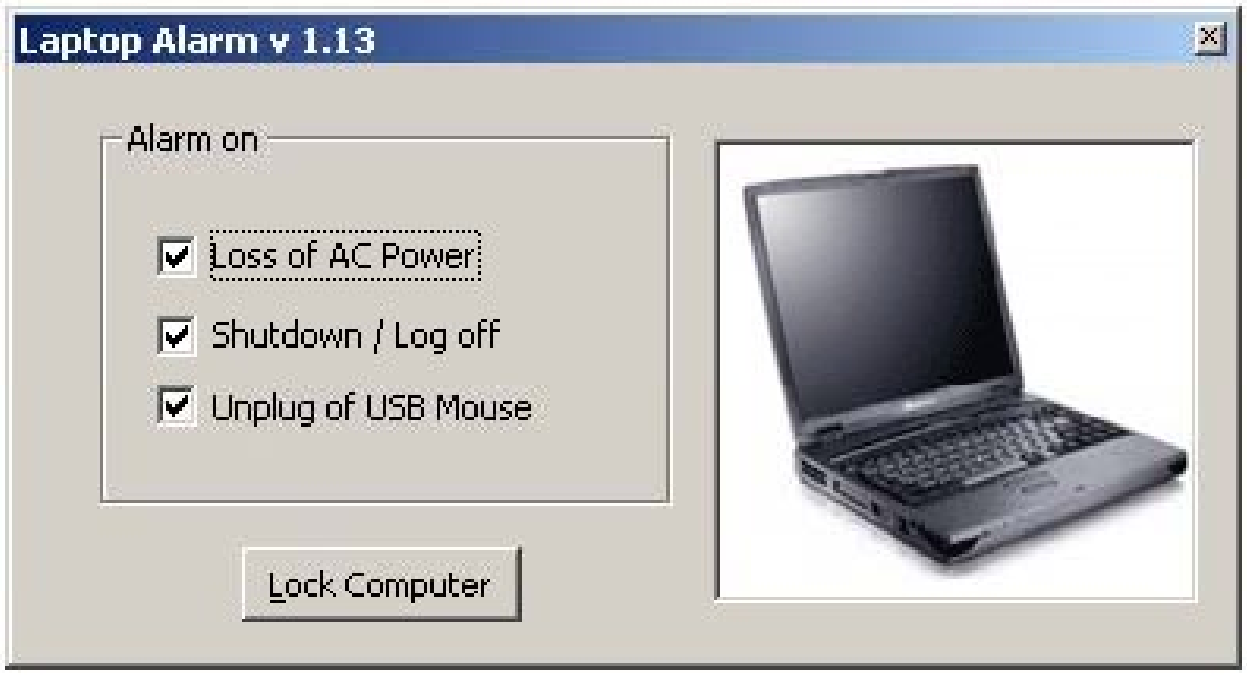
Laptop Alarm

Laptop Alarm will emit a loud alarm whenever someone tries to steal your laptop

It emits the loud sound on

- A/C Power Removal
- Mouse Removal
- Mouse Movement
- Shutdown / Suspend

Laptop Alarm: Screenshot



Flexysafe

Flexysafe is the laptops safe security case

Flexysafe Digital, the safe that is designed for people who take their laptop computers home from work

Master Lock

Master Lock patented lock and cable system

Features

- Locks notebook computer to prevent theft and protect data
- Galvanized steel cable provides strong security and peace of mind

eToken

eToken represents the most effective combination for protecting data on your laptops

It is a strong authentication, with disk encryption and boot-protection solution

A smart card-based strong authentication solution ensures PC and laptop security with two key components

- Physical protection of the encryption keys
- User authentication prior to encryption key access

STOP-Lock

STOP-Lock combines tracking system with a locking mechanism to help deter thieves

It is a highly-visible small metal plate that attaches securely to the cover of the laptop

The plate is stamped with unique barcode information that registers the computer with a national database

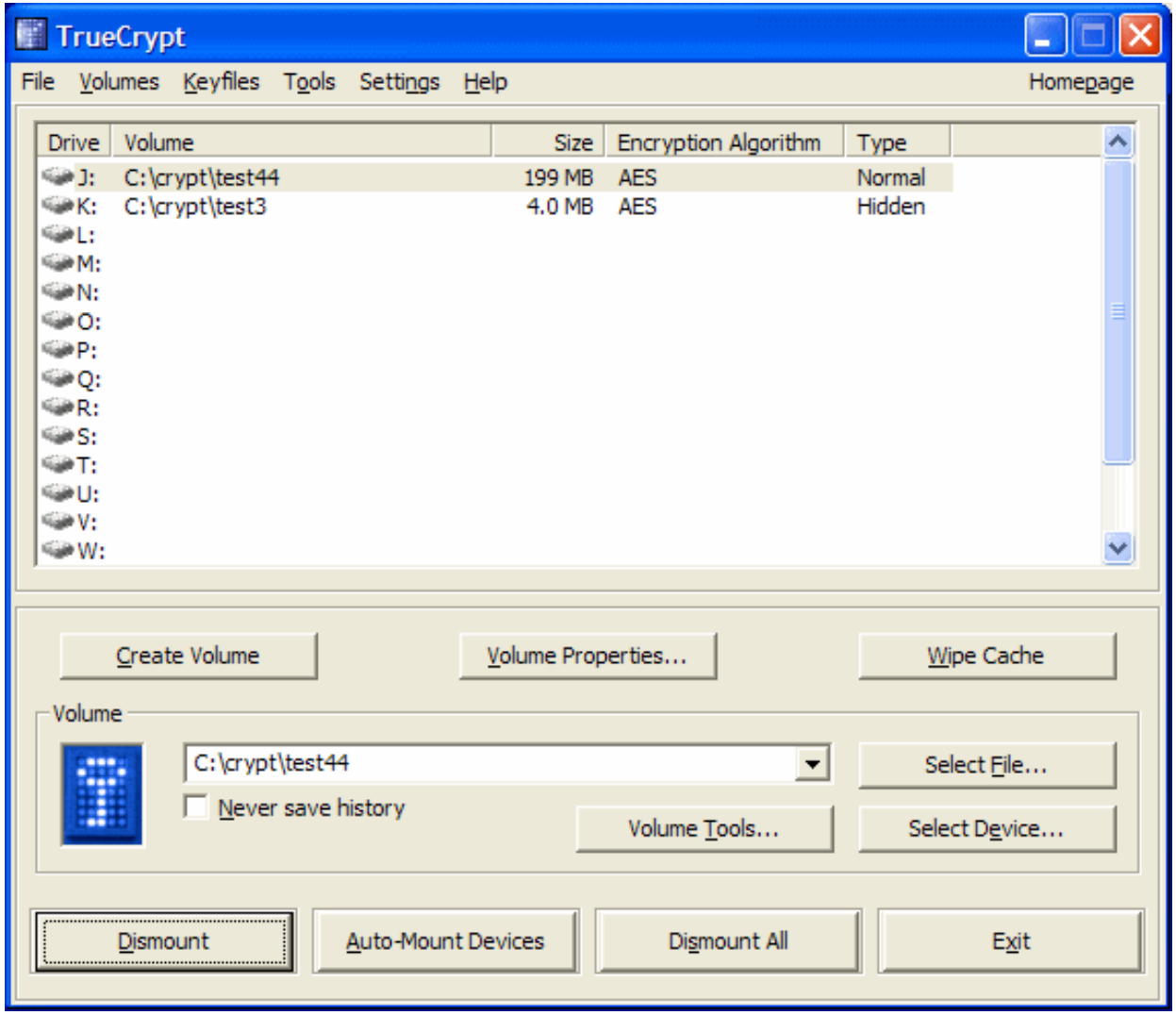
True Crypt

Free open-source disk encryption software

Features

- Creates a virtual encrypted disk within a file and mounts it as a real disk
- Encrypts an entire partition or storage device such as USB flash drive or hard drive
- Provides two levels of plausible deniability, in case an adversary forces you to reveal the password
  - No TrueCrypt volume can be identified
  - Hidden volume (steganography)

True Crypt: Screenshot



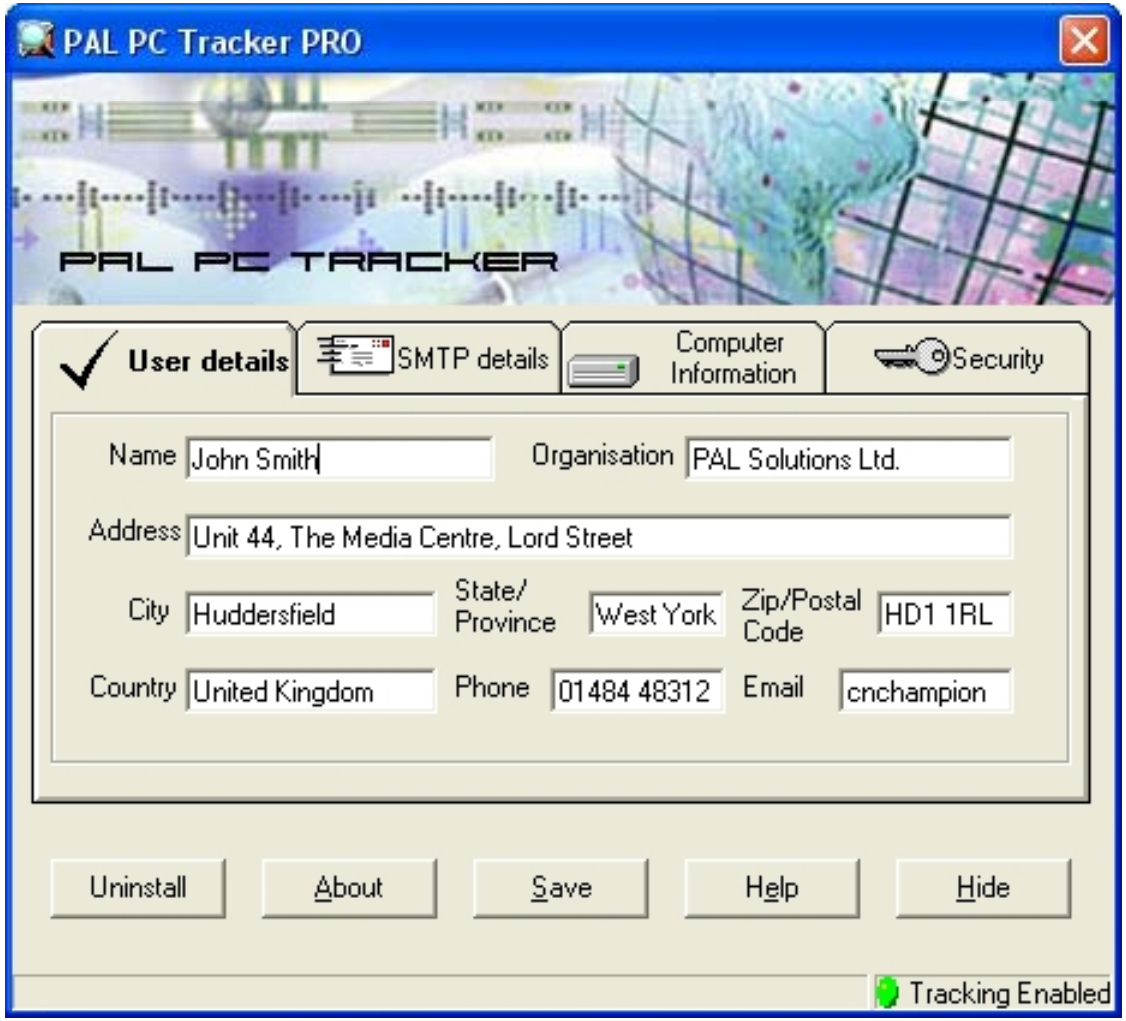
PAL PC Tracker

PAL PC tracker will track and locate the lost or stolen computer

It sends stealth signal which include the user's computer tracing details

When the user connects to the Internet, it will send a stealth email message to the user and server which contains exact location of the pre-defined email address set by the user

PAL PC Tracker: Screenshot



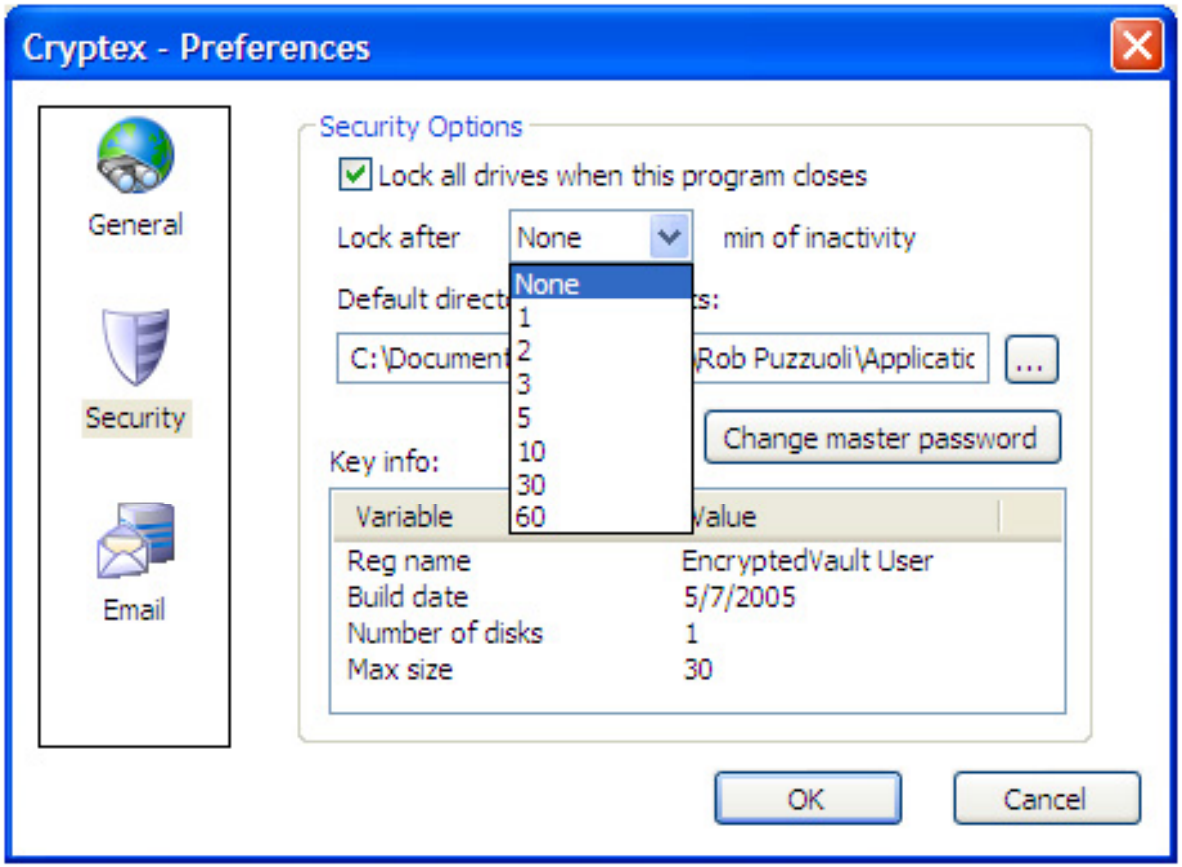
Cryptex

Cryptex provides an unbreakable, 448-bit encryption data storage on laptops

It keeps the data safe by creating an encrypting vault on the hard drive

It will disappear from the view when the vault is locked

Cryptex: Screenshot

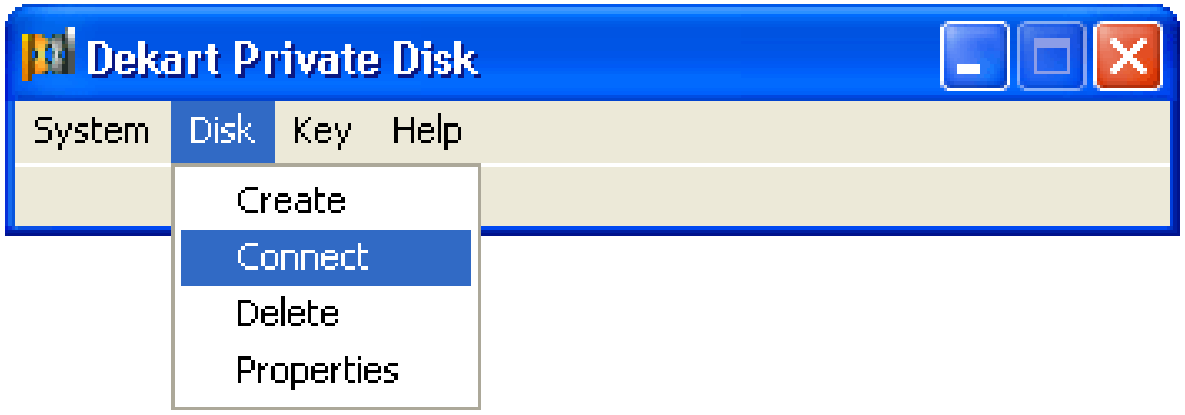


Dekart Private Disk Multifactor

Private Disk Multifactor is a disk encryption program that secures confidential data on laptops

It provides proactive protection against viruses, Trojans, adware, spyware, and unauthorized network access

Sensitive data is not only encrypted, but are protected with Dekart's innovative Disk Firewall mechanism



Laptop Anti-Theft

Laptop Anti-Theft recognizes and traces through both internal and external networks for LAN/WAN configurations to pin point actual location of the lost or stolen laptop

Once installed invisibly on your laptop system, Laptop Anti-Theft sends a stealth e-mail message containing it's exact location to a pre-determined e-mail address set by the owner

Each signal contains all the required information on the status and physical location of your laptop

Inspice Trace

Inspice Trace is a location tracking program that emails you the precise location of your stolen or lost laptop

It lets you unrecoverably destroy sensitive data in your laptop in case of theft

ZTRACE GOLD

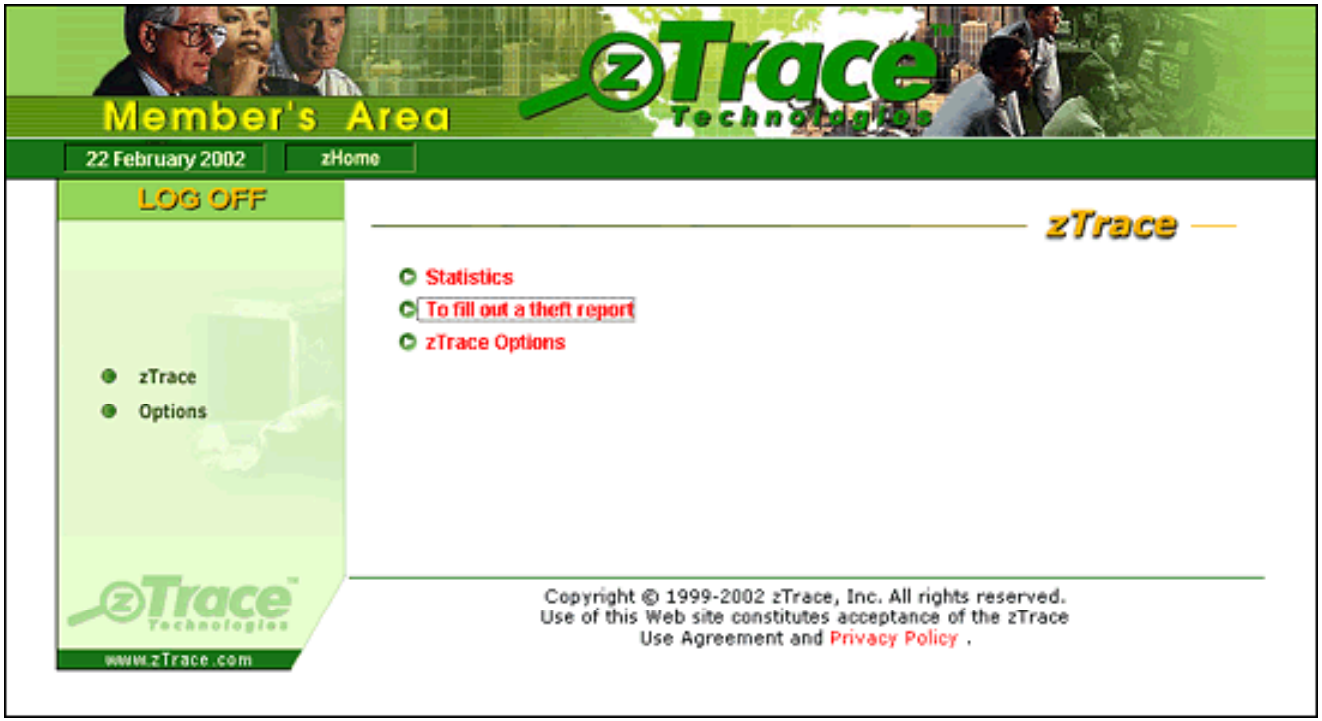
ZTRACE GOLD is an invisible software security application that traces the location of missing laptops for recovery

It is undetectable and unerasable on a laptop's hard drive

If the laptop is reported missing, a patent pending process occurs for the ZTRACE Recovery Team to identify the computer's exact physical location

The ZTRACE Recovery Team coordinates with local law enforcement for a completely outsourced recovery solution

ZTRACE GOLD: Screenshot



SecureTrieve Pro

SecureTrieve Pro is a software tool that encrypts, protects and retrieves critical files from a lost or stolen laptop

It automatically retrieves critical files remotely from your missing laptop

It offers very powerful encryption capabilities

It goes through firewalls to find the exact location of your stolen laptop

XTool Laptop Tracker

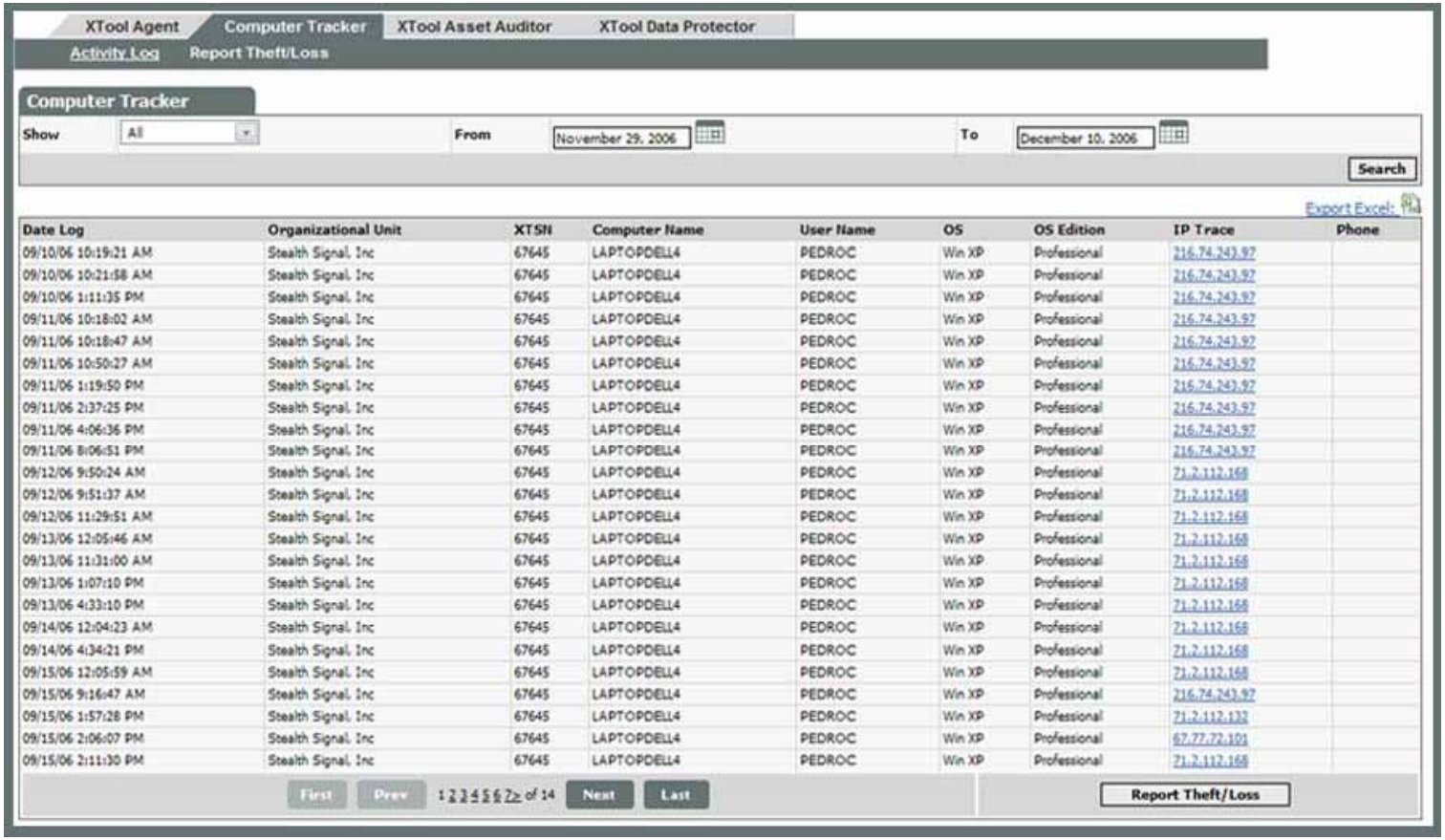
XTool Laptop Tracker supports all the recovery methods: Internet, Caller ID, WiFi, WebCam, GPS, Remote Forensic Tools

It cannot be detected by anti-virus programs and can bypass 90% of all corporate and personal firewalls

XTool Laptop Tracker Agent is small and uses encryption to transmit the collected data to the XTool Monitoring Center

It utilizes worldwide Internet monitoring and unique dial-up monitoring coverage

XTool Laptop Tracker: Screenshot



XTool Encrypted Disk

XTool Encrypted Disk is a centrally managed proactive remote laptop security solution

It ensures the intellectual property, important information and confidential data stored on your remote laptops is secure

Protect remote users from data security threats by encrypting sensitive information and preventing unauthorized access to important and confidential files

Define alerts to enforce data security policies

XTool Encrypted Disk: Screenshot

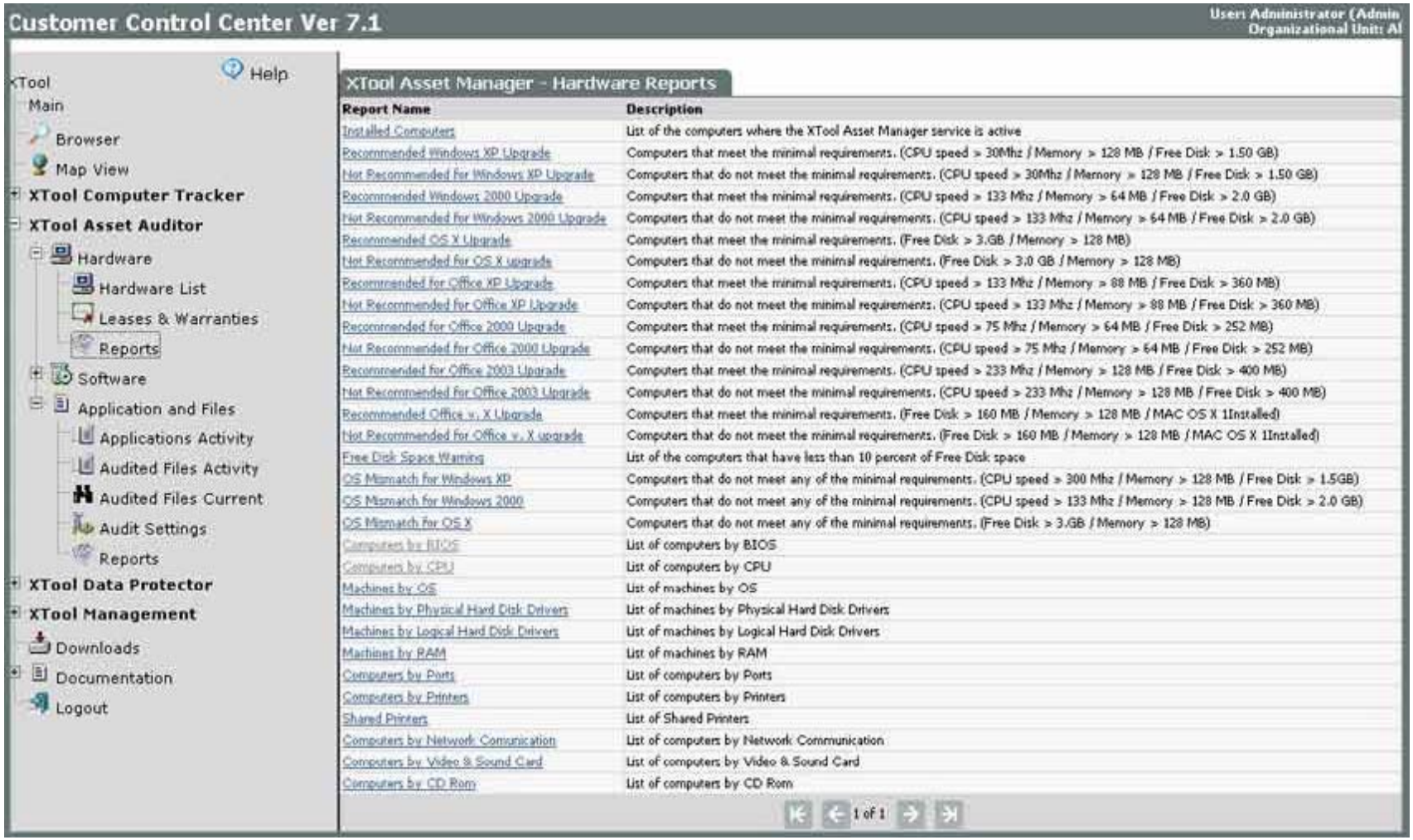
XTool Asset Auditor

XTool Asset Auditor is a centrally managed auditing service

It uses a low bandwidth agent to remotely collect information about hardware components, software installed and application usage

The zero-touch auditing solution makes keeping track of your mobile computer's hardware and software contents effortless and available no matter where they travel

XTool Asset Auditor: Screenshot



XTool Remote Delete

The XTool Remote Delete enables users to remotely and securely delete sensitive data to prevent unauthorized access to important and confidential files

It minimizes data security breaches

It provides a feedback that confirms what files were found and deleted from the target computer

XTool Remote Delete: Screenshot

Countermeasures and Security

Securing from Physical Laptop Thefts

Use Remote Laptop Security to prevent access to the secured data

Use a docking station

- Docking station permanently affixes the laptop to the desktop and also locks the laptop securely at one place

Eject the PCMCIA NIC cards when the laptop is not in use

Use a personal firewall to the laptop

Use security gadgets like motion detection and alarms to alert you when the laptop is moved by a third party

Use tracking software to trace the laptop using traceable signals when the laptop is lost or stolen

Hardware Security for Laptops

Security cable locking devices fix the laptop to an immovable object

Cable alarms alert the user at the time of malicious activities

Key lock locks down the laptop to the surface where it is most used

A remote control storage case is used for the laptops to protect from thefts

Protecting the Sensitive Data

- Use the NTFS file system which provides file level security and protects from laptop thieves
- Disable the Guest Account
- Rename the Administrator Account
- Consider creating a dummy Administrator account
- Prevent the last logged-in user name from being displayed
- Enable EFS (Encrypting File System)
- Disable the Infrared Port on the laptop
- Backup the data before leaving
- Consider using offline storage for transporting sensitive documents

Preventing Laptop Communications from Wireless Threats

- Enabling Wired Equivalent Privacy (WEP) / Wi-Fi Protected Access (WPA) on the wireless network
- MAC address control allows the wireless connections from MAC card whose MAC address is stored in the filter
- End to end encryption where the conversation is in the encrypted mode
- VPN (Virtual Private Network) protects the information transmitted over wireless links
- Access points evaluation checks for any rogue access points in wireless networks

Protecting the Stolen Laptops from Being Used

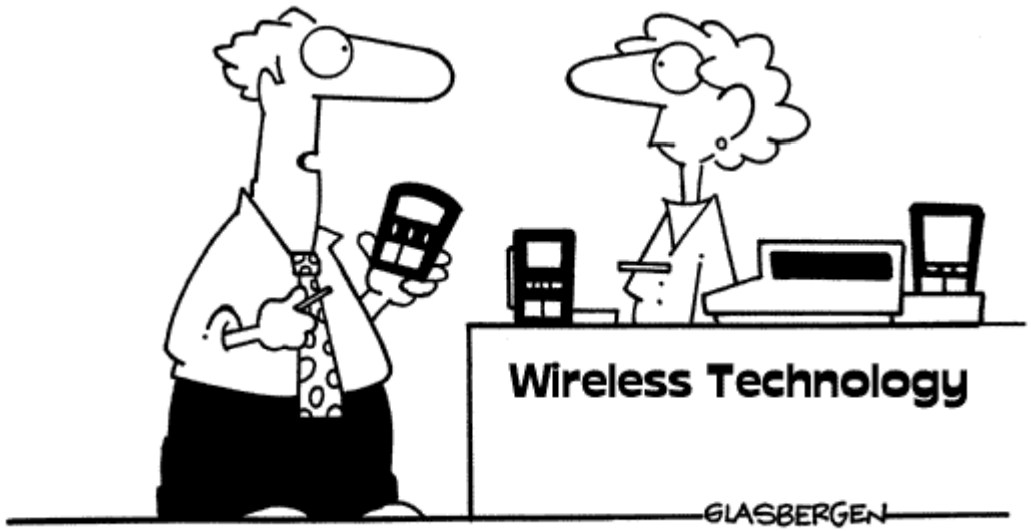
- Set the BIOS password which prevents the machine from continuing with the operations when the password is incorrect for three consecutive attempts
- Set Login password to successfully login to the computer
- Encrypting the file system
- Use Biometric authentication mechanism (such as, fingerprint reader, face reader, retinal pattern reader etc.)
- Use of tracing and tracking software's

Security Tips

- Install anti-virus software and firewalls
- Use cable locks on laptops as visual deterrents
- Use asset tracking and recovery software
- Invest in advanced data protection
- Back-up valuable data on a scheduled basis
- Keep laptops unnoticeable
- Avoid leaving unsecured notebooks unattended
- Encrypt your data
- Never leave access numbers or passwords in your carrying case
- Use alarm bells
- Lock unwanted ports

Summary

- Criminals target laptops for quick profits and misuse of the confidential data
- Interception and monitoring wireless traffic through various sniffer tools and interception software
- MAC address control allows the wireless connections from MAC card whose MAC address is stored in the filter
- WPA is used as an extensive level of security for wireless LAN's
- Face Recognition technology is used to access the laptop by recognizing the face as the password



"While I'm sending e-mail, trading stocks, and communicating with clients, my feet are just wasting time. What have you got to make my feet more productive?"

"Watch where you're going, Larry — you walked right through my wireless data stream!"