CYBER SOLUTIONS FOR THE FIGHT AGAINST CRIME
FinFisher™ partners exclusively with Law Enforcement and Intelligence Agencies, being your reliable IT partner and trusted advisor to effectively prevent and investigate terror & crime. It is privately owned with worldwide presence and proven track record serving top clients in the Law Enforcement and Investigation arena.
SECTION A
Tactical Intelligence Gathering
06 Leo5 TIDE
08 Leo5 Mobile TIDE

SECTION B
Strategic Intelligence Gathering
10 RMS PC
11 RMS Mobile

SECTION C
Deployment Methods & Exploitation
13 LOCAL DIVER
14 LAN DIVER
15 NET / ISP DIVER
16 WEB DIVER
17 XPL DIVER

SECTION D
19 Cyber Intelligence Training & Consulting

SECTION E
21 Intelligence Support
Cyber Solutions For The Fight Against Crime

FinFisher™ Solutions

Company
Founded in 2007 in Germany, with the mission to be your reliable IT partner and trusted advisor to effectively prevent and investigate terror and crime.

Tactical Intelligence Gathering
Helps your organization in profiling serious criminals and assists in the collection of target related information.

Strategic Intelligence Gathering
FinFisher™ offers a strategic wide-scale interception and monitoring solution that is device independent.

Remote Monitoring & Deployment
FinFisher™'s Remote Monitoring Solution covers the latest PCs, smartphones, tablets and most common operating systems.

Training & Consulting
FinFisher™'s Training Academy offers certified customized trainings and qualified support, thus setting the basis for every successful investigation.

Intelligence Support
The Intelligence Support sustains upgrades and updates of the FinFisher™ product line in combination with an annual support contract.
FinFisher™ is a solutions suite in the field of IT Investigation that helps your organization in investigating serious criminals and assists in collecting, processing and analysing target related information.

**Tactical Intelligence Gathering**
- Network interception & deployment solution
- Covert operational appliances

**Strategic Intelligence Gathering**
- Government grade Remote Monitoring Solution
- Suited for PC, Notebooks, Smartphones & Tablets
- Vast array of features depending on the Operating Systems

**Deployment Methods & Exploitation**
- Physical Deployment
- Tactical Deployment
- Strategic Deployment

**Cyber Intelligence Training & Consulting**
- Cyber Intelligence Basics
- Cyber Intelligence Programme
- Team Build Up & Development
- Operational Support

**Intelligence Support**
- Regular updates and upgrades
- Professional back-office support for problem solving and technical queries

---

**Intelligence Cycle**
- Planning & Direction
- Target and Objective Definition
- Information Gathering
- Processing and Collation of Information
- Intelligence Analysis and Production
- Intelligence Information Dissemination
- Reassessment

---

03
The trends in today’s communication technology are based on a few simple facts:

- Mobility of the user
- Based on IP data
- Service and usage
- Higher security standards

These trends restrict traditional investigational methods & interception technologies, so much that the efficiency and results of cyber investigations are severely diminished.

Furthermore the threat patterns caused by terrorism and organized crime have developed to higher complexity and aggression due to the availability of technology and know-how transparency through the internet.

On the other side there are the trends in the surveillance and intelligence industry to counter such tendencies. In terms of target-based investigation there is a shift from a ‘strategic interception’ approach to a more ‘tactical’ methodology by utilizing devices and environmental monitoring.
SECTION A

Tactical Intelligence Gathering

06 Leo5 TIDE
08 Leo5 Mobile TIDE
Leo5 TIDE

'Leo5 TIDE' is the latest innovational step in IT Investigation Software created by FinFisher™ - a Tactical Monitoring Solution for Wi-Fi and Local Area Networks, combined into one package providing a diverse set of functionalities.

It has been built to seamlessly integrate with the current and future Remote Monitoring Solution architecture, to support, improve and compliment the wide range of tasks that are essential to Law Enforcement in their day-to-day operations. Leo5 TIDE brings you the capability of acquiring a vast array of important data, collected from in-field deployed sensors that can be remotely controlled by operatives from a central facility.

As with all our products, we have worked to ensure that all complex techniques have been implemented to provide a simple and efficient usage to enable the user to focus on what matters: Discovering and recording evidence to locate and convict criminals.

Features

Leo5 TIDE brings several new core functionalities to RMS, giving you a higher level of control of the data you collect and manage:

- Sensor Management: Configure and remotely control your Leo5 TIDE sensors to get the data you need.
- Data Management: Download and manage the data collected from multiple sensors.
- Data Analysis: Easy-to-use analysis of recorded data by all deployed sensors.

All of this is accessed by the user from the Headquarters Control Centre.
Operational Scenarios

Session Hijacking

The Tactical devices can record a target’s HTTP traffic and extract necessary information, like session ID/cookies and hijack his active sessions without the knowledge of any login credentials. A logout request of the target will be canceled to keep the session ID/cookie data valid.

Multiple Location Monitoring

Due to its modular structure, the end user can position various devices in strategic locations and monitor target movements and profile his activities.

Remote Deployment

FinFisher™ has implemented a remote deployment module into Leo5 TIDE. This allows the end user to remotely redirect target’s traffic using MitM attack (fake access point) thus, providing devices with a solid deployment solution. This can be achieved via Web-deployment of 1 or 0 day exploits or download deployment to cite a few examples.
Leo5 Mobile TIDE

The Leo5 Mobile TIDE is a cutting-edge surveillance product that has been created in close cooperation with intelligence units from various countries in order to create a powerful, covert and easy-to-use product for Law Enforcement Agencies.

It provides a wide-range of features for undercover operations from gaining access to Wi-Fi networks, detecting and monitoring Wi-Fi clients, jamming devices and networks, silently recording all network traffic and extracting account credentials for logins of various applications such as Browsers or E-mails.

Leo5 Mobile TIDE Features

**Wi-Fi Scanner**
- Detect Wi-Fi Networks
- Identify all clients for each network
- Identify unassociated clients
- Identify clients’ preferred networks

**Wi-Fi Cracker**
- Recover WEP Encryption keys within minutes
- Automated WPA password recovery

**Wi-Fi Jammer**
- Jam complete Wi-Fi networks and individual clients

**Wi-Fi Catcher**
- Provide specific open Hot-Spot
- Supports “Capture All” Mode
- Internet Access through Wi-Fi or Mobile Data

**Network Monitoring**
- Automated “Man-in-the-Middle” attack
- Detect network vulnerability
- Full Browsing History and Account recording

**SSL - TLS interception**

**Data Analysis & Reporting**

**Deployment techniques in combination with XPL DIVER**

*Leo5 Mobile TIDE proven in action*

**The pedophile**

Police found out about a local pedophile but lacked evidence to convict him. They suspected he was conducting unlawful activities from his home-based computer.

Parked outside his house, the police decoded the WPA encryption of his wireless network with the Leo5 Mobile TIDE. From headquarters, they monitored his webmail and social media activities. Three days later the suspect was arrested.

**The unlawful traveler**

Special agents were following a suspect but couldn’t get physical access to his notebook. He regularly used WLAN at the coffee shop, in his hotel room, in the lobby and at the airport. Watching him with the Leo5 Mobile TIDE appliance, an agent blocked his WLAN access. The agent’s notebook appeared in the suspect’s WLAN options when he tried to regain access. Unknowingly, the suspect connected his notebook to the agent’s, which let him obtain all information sent through the network like passwords and emails.
SECTION B

Strategic Intelligence Gathering

10 RMS PC
11 RMS Mobile
RMS PC

RMS PC is a field-proven Remote Monitoring System that enables law enforcement and investigation organizations to face the current challenges of monitoring mobile and security-aware targets that regularly change location, use encrypted and anonymous communication channels and travel internationally.

When RMS PC is installed on a computer system it can be remotely controlled and accessed as soon as it is connected to the Internet, no matter where in the world the system is located.

RMS PC Features

- Covertly transmits data to headquarters
- Allows live remote forensics of targeted systems
- Records target’s communication activities like emails and chats
- Monitors VoIP calls, chats, videos, contacts and file transfers
- Executes live surveillance through webcam, microphone and screen
- Traces the target location in every country
- Uses advanced filters to record only relevant information
- Supports most common operating systems (Windows, Mac OSX and Linux)
- Bypasses almost 35 regularly tested Antivirus systems
- Delivers valid evidence in compliance with international laws and regulations
- Fully integrates into law enforcement monitoring functionalities
- Allows agents to receive different user rights according to security clearances
- Makes use of anonymising proxies to avoid public detection
- Extracts username & password combination for various application such as browser, messengers or social media

RMS proven in action

Drug cartel meetings

Several covert agents had failed to enter the inner circle of trust of an organized crime group providing drugs to a vast region of the city.

Instead, they managed to deploy RMS PC on the computer systems of some members of this group. Using the country tracing and remote microphone functionalities, essential information could be gathered from every meeting that they held.
RMS Mobile

RMS Mobile is a field-proven Remote Monitoring System that enables law enforcement and investigation organizations to face the current challenges of monitoring mobile and security-aware targets that regularly change location, use encrypted and anonymous communication channels and travel internationally. RMS Mobile is a very attractive solution for customers with limited access to mobile network infrastructure, as it allows them to monitor mobile phones with enhanced capabilities.

When RMS Mobile is installed on a mobile phone it can be remotely controlled and monitored no matter where in the world the target is located.

**RMS Mobile Features**

- Covertly transmits data to headquarters
- Records target's communication activities, like calls, SMS, MMS, emails and chats
- Downloads contact, calendar and picture files, even if they are not transmitted over any network
- Executes live surveillance of mic, webcam and screen
- Traces the target's location in almost every country through GPS and Cell ID
- Offers access to encrypted communications, e.g. messengers, emails or PIN messages
- Uses advanced filters to record only relevant information
- Supports most common mobile operating systems: Android, iOS & BlackBerry
- Delivers valid evidence in compliance with international laws and regulations
- Fully integrates into law enforcement monitoring functionalities
- Allows agents to receive different user rights according to security clearances
- Makes use of anonymising proxies to avoid public detection

**RMS Mobile proven in action**

**Organized crime gang**

A team of investigators had targeted an organised crime gang, whose leader was aware of the government's electronic surveillance techniques and therefore advised the gang members to be very careful. The investigators profiled the gang and identified an individual who might be susceptible to social engineering influences.

The individual was informed about a certain "hidden" App (containing the Remote Monitoring Solution), supposedly designed to bypass all forms of governmental electronic surveillance, thus making communication secure. This App was promoted to the gang leader, who then instructed all members to use the App as default means of communication.
SECTION C

Deployment Methods & Exploitation

13 LOCAL DIVER
14 LAN DIVER
15 NET/ISP DIVER
16 WEB DIVER
17 XPL DIVER
LOCAL DIVER

The LOCAL DIVER is a complete tactical solution that can be used and deployed in the field by Law Enforcement Agencies. It is a powerful, covert and easy-to-use physical product suite that enables unlocking devices such as computers and mobile phones as well as covert deployment of monitoring software. It combines five functionalities:

- Mobile Deployer
- Mobile Unlocker
- Mobile USB Deployer
- PC Covert Cable
- PC USB Deployer

LOCAL DIVER Features

Mobile Deployer
- Tactical, fast rooting / jailbreaking & deployment solution
- Covertly roots / jailbreaks
- Deploys a pre-configured payload
- Supports iPhones and various Android phones

Mobile Unlocker
- Automatically brute-forces 4- to 6-digit
- Provides valid PIN number on successful recovery
- Supports Android

Mobile USB Deployer
- Automatically displays installation files on connection
- Provides simple deployment
- Supports Android

PC Covert Cable
- Covert device for undercover operations
- Agent controlled deployment through covert RF device
- Supports Windows, OSX and Linux

PC USB Deployer
- Runtime and Boot installation
- Simple and quick installation within 10-30 seconds
- Supports Windows

LOCAL DIVER proven in action

Technical surveillance unit

The LOCAL DIVER was successfully used by technical surveillance units in several countries to deploy remote monitoring solutions onto target systems that were switched off by simply booting the system from the LOCAL DIVER USB device. This technique worked even for target systems that were equipped with full hard-disk encryption.
LAN DIVER

Some of the major challenges law enforcement agencies face are mobile targets that don’t allow any physical access to their computers and don’t open any unknown files they receive. Security-aware targets are almost impossible to monitor as they keep their systems up-to-date and successfully resist common exploits or intrusion techniques.

LAN DIVER covertly deploys Remote Monitoring Solution (using MITM technique) on target systems in Local Area Networks (wired and wireless). It patches files that are downloaded by the target on-the-fly, sends fake software updates and deploys the monitoring solution into visited websites.

**LAN DIVER Features**

- Discovers all computer systems connected to a Local Area Network
- Works in wired and wireless networks
- Deploys a remote monitoring solution in downloads of targets
- Injects remote monitoring solution as a software update
- Remotely installs a remote monitoring solution through websites visited by the target

**LAN DIVER proven in action**

*Terrorism case after severe attack happened in the country*

Investigators performed a Man-in-the-middle (MITM) attack to a known target in a big hotel. Hotel management provided access to a room near to the suspect’s room and through the use of a IMSI catcher the phone number was extracted.

The investigator called the obtained number and verified the suspect’s identity.

The data collection allowed to prepare a personalized software package with RMS for the suspect’s device.
NET/ISP DIVER

In many real-life operations, physical access to targeted systems cannot be achieved. To solve this, a covert remote installation of a remote monitoring solution is required.

NET/ISP DIVER is a tactical/ portable solution to be deployed in a “friendly” LAN environment on short notice. This could be in hotels, hot spots or companies where the customer has the support of the network owner. This can also be achieved at ISP level using Policy Based Routing (PBR) approach. Via LAN a remote monitoring solution can be remotely installed on selected target systems.

NET/ISP DIVER is based on a high performance portable PC combined with a management notebook to provide maximum mobility and flexibility in the targeted networks.

A wide range of network interface cards, all secured with bypass functions, is available for the required active network connectivity. The end-user can select several sophisticated passive methods of target and traffic identification. Each method can be used either stand-alone or combined, to provide maximum success in identifying the targets of interest. Files that are downloaded by the target on-the-fly, combine the deployment methods making use of the XPL DIVER; thus, enhancing the deployment chances or install the solution through websites.

NET/ISP DIVER Features

- Can be installed inside a LAN environment (e.g. in a hotel, hotspot or company)
- Works with Ethernet (1000Base-T, 1000Base-SX, 1000Base-LX), VLAN support
- Identifies targets using different passive profiling and identification methods
- Deploys a remote monitoring solution as a software update and provides enhanced deployment capabilities through the use of the XPL DIVER
- Installs a remote monitoring solution through websites visited by the target
- Performs IP Monitoring (PCAP files)

NET/ISP DIVER proven in action

Secret service

NET/ISP DIVER was deployed in a hotel’s LAN in front of the DSL modem before the IP-traffic was transmitted to the Internet Service Provider’s network. Targets of interest could be identified in the IP-traffic by various passive profiling and identification methods and the remote monitoring solution was deployed on the positively identified target systems. In parallel, it is possible to perform IP Monitoring since we are sitting in the middle of the traffic.
WEB DIVER

One of the major challenges in investigative monitoring is to install a solution onto a targeted system; especially when only a little information, like an email address, is available and no physical access can be achieved.

WEB DIVER is designed to provide remote and covert deployment on a target system by using a wide range of web-based attacks.

WEB DIVER enables the investigator to covertly install Remote Monitoring Software onto Target Systems through Websites. It generates a wide-range of attack codes that can be implemented into given websites providing the Remote Monitoring software for download when visiting such websites.

WEB DIVER Features

- Comes with customizable web modules
- Installs itself into every website
- Can be integrated with LAN DIVER and NET/ISP DIVER to be deployed even via popular websites like webmail or video portals
- Is easy to use thanks to a point-and-click interface

WEB DIVER proven in action

The frequent internet user

After profiling a terrorist and getting to know his online behavior, a technical surveillance unit created a website that would interest him and they sent him the link via a discussion board. Upon opening the hosted website the WEB DIVER code provides the Remote Monitoring solution for download on the terrorist’s system. After installation the system can be monitored from within headquarters.
XPL DIVER

XPL DIVER is FinFisher™'s sophisticated online system to easily select, configure and use Exploits and useful Intrusion tools.

The infrastructure of XPL DIVER is implemented with high security measures:
- Relays for Portal access
- Encrypted communications between all entities for all data exchange processes
- Maximum security given to the transmission channels and packages
- Upon expiry of an Exploit, all stored data will be deleted

XPL DIVER Features

- Portal with exclusive client access residing in own infrastructure
- User-friendly GUI to generate the Exploits & payload
- Provisioning of secure relay software for communication (Exploit & generation)
- Availability of 2 major yearly releases and 3 – 5 Premium Exploits

XPL DIVER proven in action

High-tech crime unit

A high-tech crime unit was investigating a cybercrime and needed to deploy a remote monitoring solution on a target system. They used an Adobe Acrobat Reader 0-day exploit and sent the target a prepared file via email. The remote monitoring solution was automatically deployed once he opened the file.

Intelligence agency

A target was identified within a discussion board but no direct or email contact was possible. The agency created a web server containing an Internet Explorer 0-day exploit, which deployed the solution on the target system after he opened the URL that was sent to him through a private message in the discussion board.
Cyber Intelligence Training & Consulting

You have come to know FinFisher™ as the leading provider of cyber intelligence solutions tailored for the unique challenges of the law enforcement and intelligence space.

We have developed the products that meet your requirements in close cooperation with our customers, and directly implemented additional features in direct response to their requests.

We have realized some clients not only need ‘basic or advanced training’ but a more solid and comprehensive approach. Our new program offers a comprehensive and updated approach in terms of know-how transfer and response to clients' specific training needs from scratch.

On the other hand we want to focus on consulting our valued clients and walk along until a solid Cyber-team is formed and operating. Once that is completed, we will continue to provide our services in the form of 'operational support and consulting'.

**CYBER INTELLIGENCE BASICS**

This training path replaces the IT Intrusion Training range of trainings. Courses are generally held over the space of five consecutive days either at your facilities, in-country - or at one of our facilities in the different regions where we are present.

We do not believe in lectures. Course topics are instead drawn from that week's IT security headlines, our trainers' vast background knowledge, lots of hands-on course contents and a Capture the Flag (CTF) challenge at the end of the course: this we believe in.

With currently nine distinct training courses available and always aiming at adding extra modules/topics we are confident in our abilities to deliver the training contents you seek.

**CYBER INTELLIGENCE PROGRAMME**

To address customer demand for continued education, we are also launching the long-term Cyber Intelligence Programme. The FinFisher™ CIP is structured to meet the one customer requirement that we have observed as becoming more and more prevalent in the recent years: the mentored approach to recruiting and building teams with cyber security capabilities, coupled with ongoing training based on recurring evaluation.

Our experts will work closely with you to evaluate your current team setup. Existing strengths and areas for development will be identified, and you will receive bespoke training offers tailored to your unique assets and requirements.
SECTION E

21 Intelligence Support
Intelligence Support

The Intelligence Support sustains upgrades and updates of the FinFisher™ product line in combination with an annual support contract.

The FinFisher™ Support Team provides the following services to our clients:

Access to:
- Latest user manuals
- Latest product specifications
- Latest product training slides
- Latest Antivirus test reports

Regular Software Updates:
- New features
- New major versions
- Bug fixes

Technical Support:
- Partial operational support
- Bug fixing

Lifeline Support

The Lifeline Support provides professional back-office support for problem solving and technical queries. It also provides back-office support remotely, for FinFisher™ software bug fixes and hardware replacements under warranty. Furthermore, with Lifeline Support the client automatically receives new features and functionalities with each release.

Software Upgrades

The Lifeline Support includes regular software upgrades and guarantees automatic upgrades to the existing system with software patches provided via the update system.

These upgrades include new features, new enhancements and new functionality (excluding hardware).