OPENLI FAQ

1. ***What is OpenLI?***

   OpenLI is a lawful interception software solution written by the WAND Network Research group at the University of Waikato. OpenLI implements the ETSI standards for the interception of IP and IP multimedia services.

   The initial development of OpenLI was funded by a group of New Zealand Internet service providers. The primary aim of OpenLI was to meet the requirements of New Zealand's TICSA legislation, which required network operators to deploy an ETSI-compliant LI system into their networks.

2. ***How does the OpenLI lawful intercept architecture work?***

   An intercept begins with a law enforcement agency serving a warrant to a network operator. The warrant contains the key parameters for the intercept. Using the information in the warrant, the operator will tell OpenLI to commence the intercept by updating the running intercept configuration on the OpenLI provisioner. Usually, the operator would do this by sending the details of the new intercept to the provisioner using a REST API.

   The provisioner is the central controller of an OpenLI system – there is only ever one provisioner in a deployment and is the only OpenLI component that an operator should need to interact with during normal operation.

   The collectors are the components that perform the actual interception of communications to/from the intercept targets. The provisioner sends intercept instructions to the collectors that describe how to recognize the communications for the current set of intercept targets, as well as any additional tags that need to be included with each intercepted communication.

   The collectors must be provided with a feed of potentially interceptable communications by the operator. Often, this is a “mirrored” copy of the communications data seen at a router in the core of the operator network. We leave the exact specifics of how to get the communications into the collectors up to the operator, as the best method will vary depending on the structure of their network and the type of communications that they are willing to intercept.

Operators may have presence in multiple physical locations, and they may need to deploy multiple OpenLI collectors (one for each location) – supporting multiple separate collectors is an important feature of our architecture. Multiple collectors may also be used for load balancing purposes.

Each collector looks at the mirrored communications it receives and checks to see if it should be intercepted. If interception is required, then the communication is copied and encoded into the corresponding ETSI record format. The encoding is very important – simply intercepting communications is easy, but the ETSI format is complicated and requires special software (like OpenLI) to be able to implement. The encoded record is then passed on to the mediator.

The mediator is effectively the exit point of an OpenLI deployment – it collects the encoded intercept records from the collectors and ensures that they are delivered to the law enforcement agency that requested them. The provisioner tells the mediator which intercepts belong to which agency. The mediator sends the records to the correct agency over some form of encrypted tunnel.

Most deployments only have one mediator, but it is possible to have more than one mediator if necessary (e.g., if you are running a lot of intercepts for some reason and need to spread the mediator workload across multiple devices).

3. *What level of support is available?*

Often our customers need prioritized support and extra attention to solve critical issues. To help our clients, we offer low-cost paid support subscriptions. These are renewable and give you access to on demand software support via various channels. To get a quote for your business, send us a message using the contact form on our website.

4. *What differentiates OpenLI's lawful interception solution?*

OpenLI is the world's first and only (to date) open-source lawful interception solution. OpenLI enables smaller network operators to meet their lawful interception obligations for a fraction of the cost of a commercial alternative. OpenLI supports the ETSI standards for lawful interception that are used in many countries throughout Europe, Asia, Oceania and many other parts of the world, and has been successfully deployed by a number of network operators in New Zealand.

5. *Which ETSI standards does OpenLI implement?*

OpenLI implements the following ETSI standards:
ETSI TS 101 671 (v3.12.1)
ETSI TS 102 232-1 (v3.5.1)
ETSI TS 102 232-3 (v3.3.1)
ETSI TS 102 232-5 (v3.2.1)
ETSI TS 102 232-7 (v3.3.1)

Adding support for the other ETSI standards, or for more recent versions of the ones that we do support is possible.

6. ***What operating systems does OpenLI support?***

   OpenLI runs on Linux only (at least for now). We currently provide binary packages for the Debian, Ubuntu, Rocky Linux, Alma Linux and Fedora distributions for easy installation and upgrading. Install instructions can be found on the OpenLI wiki.

7. ***What hardware do you need to run OpenLI?***

   Different OpenLI components have different requirements, but all OpenLI software components can be run on a commodity x86 server. OpenLI can also be run inside a virtual machine or a container, if required. Our main recommendation is that each collector node should have a DPDK-compliant NIC for packet capture; we use the Intel X520 10Gb card for development and it works extremely well. Our tutorials explain the hardware requirements for each OpenLI component in more detail, along with suggested minimum requirements for each component.

8. ***Can OpenLI interface with the lawful interception features on my existing vendor equipment?***

   For some vendors, yes. OpenLI can receive and parse the mirroring formats used by Juniper, Nokia and Mikrotik devices and convert the captured communications into the ETSI format. We will add support for other mirroring formats based on customer demand -- Cisco support should be coming soon.

9. ***Are there examples or documentation that I can use to learn how OpenLI works?***

   We have put together a comprehensive tutorial that can teach you everything you need to know to get started with OpenLI. The tutorial includes a containerized lab environment and practical exercises so you can see OpenLI working without ever having to touch your own network. The tutorials can be found on the OpenLI website. We can also deliver the tutorial as an in-person workshop for groups of interested OpenLI users -- contact us if this is something that interests you.

10. ***Is OpenLI secure?***

    We have designed OpenLI specifically to minimise the exposed attack surface. A typical OpenLI deployment is almost entirely internal to your organisation and should be easy to protect through good firewalling and security practices. More details on our security features can be found on our website.

11. ***How does OpenLI determine which traffic to intercept?***

    OpenLI parses the messages sent by session management protocols (such as SIP for VoIP, or RADIUS for IP sessions) and uses this data to keep track of which calls or data sessions belong to each network user. When a session is observed for a known intercept target, OpenLI will then intercept just the communications for that session and pass them on to the requesting authority. Any communications seen by OpenLI involving users that are not intercept targets will be immediately discarded. Note that this means that you will need to provide OpenLI with a copy of any SIP and RADIUS traffic on your network for it to be able to function correctly.

12. ***What type of customers do you support?***

    Our initial customer base is small to medium internet service providers (ISPs). OpenLI is under on-going development, and we aim to extend our customer base to larger ISPs in the near future.

13. ***Where do I direct enquiries?***

    Enquiries and questions can be directed to our team on our website or through OpenLI's support email. You can also subscribe to our newsletter on our website which is sent out to our mail list quarterly.