

# Counter Link High-Speed Collector

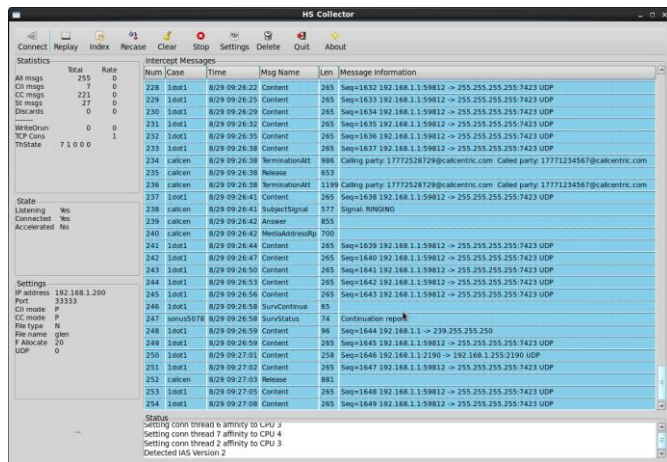


Basic lawful-interception collection system providing collection speeds above 1 Gb/s in an inexpensive form

## KEY FEATURES & BENEFITS

- Low-speed version (< 1 Gb) supplied as a software product
- High-speed version can collect at up to 4 Gb/s using 10Gb interfaces and SSD storage
- Requires no pre-provisioning; dynamically recognizes intercept cases and the LI standards in which traffic is sent
- Supports a variety of LI handover standards – ATIS, EGPP, ETSI

The HSCollector is a basic collection system that records intercepts to file storage and optionally decode and display the intercept messages on the user's screen in real time. It can run as a cloud application, an application atop a physical Linux server, or as preconfigured in a 10G system for high-speed use.



The user interface has five parts. The large window shows the decoded LI messages as they are received. The small window on the top left shows real-time statistics. The small window at the mid left shows state information. The small window at the lower left shows some of the current configuration parameters. Finally, the status window at the bottom shows status and error messages.

## Standards Supported.

The HSCollector currently supports the following LI handover standards:

- ATIS 678, versions 2 and 3
- ATIS IAS, versions 1 and 2
- ATIS-1000069, version 1
- 3GPP 33.108 EPS Part 10, versions 12 and 13 with and without the U.S. annexes G and H
- ETSI 102 232-1 and 102 232-5, versions 3.12.1 and 3.6.1

**Dynamic input recognition.** Because the LI message standards are self-describing with object identifiers and case names, the HSCollector requires no prior setup of cases. Each message sent to it is examined to determine the standard in which it is encoded and the case to which it is associated. If the case is a new case, the HSCollector recognizes it as such.

**Collection Modes.** The HSCollector is normally in collection mode, where it listens for incoming TCP connections (e-interface connections in ATIS terminology; HI2 and HI3 connections in 3GPP and ETSI terminology). In this mode, it collects all incoming information in a single file and, depending on parameters in its configuration file, parses and displays messages on the user interface. The file format can be selected to be ASN.1 BER or PCAP.

**Other Modes.** When the HSCollector is not in collection mode, the tool bar on the user interface can be used to put it in a variety of other modes, all of which are operations on a designated input file.

- **Replay mode**, in which it treats each message as if it were an incoming message, and otherwise performs the operations above.
- **Index mode**, where it lists the LI cases found in the input file.
- **Recase mode**, where it replays the input file but ignores all messages that aren't associated with a specified case. Recase can be used to segregate cases into individual files.
- **Remod mode**, where it creates a different file for each object type found in the input file.

**Message parsing.** How messages are displayed, if at all, is controlled by configuration parameters. Configuration parameters come from a configuration file but can also be changed via the user interface. During high-speed intercepts, one would disable LI message display (but the status window always displays status and error updates, including any ATIS-1000069 incoming messages). Alternatively, one can select minimal display of CII/IRI messages (basically case name, timestamp, message name), or select partial decoding/display of each message. For the latter, what is displayed

depends on the standard. E.g.,

- For the IAS standard, the IPv4 or IPv6 address associated with a new packet data session
- For IAS and 33.108, an incoming packet-data-summary message results in a table of flows, showing for each the IP addresses, ports, protocol, packet count, and byte count
- For 678 call starts, the identifiers of the calling and called parties
- For 678 signals, the signaled information
- For 33.108, the event, the IMSI, MSISDN, and MEI, and certain other fields
- For 102 232-5, the SIP message name and response code

For CC (content) messages, options are no display, parsed display (e.g., IP addresses, protocol, port), and hex display.

**TCP Analysis.** If TCP analysis is enabled, the HSCollector detects the start of each TCP connection, tracks the payload bytes in both directions, and detects the end of the connection. At the end, a “pseudo” intercept message is sent to the display containing information about the completed connection. The information displayed is the client and server IP addresses and ports, time of start, and the number of packets and total data bytes sent by both client and server.

## 10G HSCollector Physical and Electrical Characteristics



- 1U, 16.9” deep
- Approximately 16 lbs
- Operating temperature: 10-35°C
- One 1G system port (maintenance)
- One 10G port for high-speed delivery, SFP+
- Two or four SSDs, 0.8 to 4.8 TB total, 4.7 Gb/s write speed, RAID-0 striping
- AC power, typical power 90w
- Remote management via BMC/IPMI

Copyright © 2017, Counter Link LLC

Statistics	
Total	Rate
All msgs	2485 0
CI msgs	4 0
CC msgs	2351 0
SI msgs	130 0
Discards	0 0
WireCon	0 0
ThState	00000000

Num	Case	Time	Msg Name	Len	Message Information
347	CI80606	7/8 16:25:33	SurvContinue	70	
348	bob	7/8 16:25:33	SurvStatus	71	Continuation report
349	gmpc	7/8 16:26:26	SurvDeactivate	60	
350	1d01	7/8 16:26:33	SurvContinue	68	
351	CI80606	7/8 16:26:33	SurvContinue	70	
352	bob	7/8 16:26:33	SurvStatus	71	Continuation report
353	gmpc	7/8 16:26:46	SurvActivate	68	
354	gmpc	7/8 16:26:46	PDSessionEstab	303	IP address: 10.0.0.2
0	gmpc	7/8 16:27:15	*TCPDone	0	Client 10.0.0.2:59348 Server 209.234.225.242:443 Client sent 18603 bytes (48 pkts) Server sen
0	gmpc	7/8 16:27:15	*TCPDone	0	Client 10.0.0.2:59349 Server 209.234.225.242:443 Client sent 22663 bytes (57 pkts) Server sen
0	gmpc	7/8 16:27:15	*TCPDone	0	Client 10.0.0.2:59350 Server 209.234.225.242:443 Client sent 26723 bytes (68 pkts) Server sen
0	gmpc	7/8 16:27:15	*TCPDone	0	Client 10.0.0.2:59351 Server 209.234.225.242:443 Client sent 21762 bytes (50 pkts) Server sen
0	gmpc	7/8 16:27:15	*TCPDone	0	Client 10.0.0.2:59360 Server 23.3.75.33:80 Client sent 18040 bytes (27 pkts) Server sent 12180
0	gmpc	7/8 16:27:15	*TCPDone	0	Client 10.0.0.2:59361 Server 23.3.75.33:80 Client sent 20287 bytes (28 pkts) Server sent 12492
0	gmpc	7/8 16:27:15	*TCPDone	0	Client 10.0.0.2:59359 Server 209.234.235.251:80 Client sent 24584 bytes (33 pkts) Server sent
0	gmpc	7/8 16:27:15	*TCPDone	0	Client 10.0.0.2:59358 Server 209.234.235.251:80 Client sent 26790 bytes (36 pkts) Server sent
0	gmpc	7/8 16:27:15	*TCPDone	0	Client 10.0.0.2:59363 Server 4.26.67.112:80 Client sent 17102 bytes (26 pkts) Server sent 1811
0	gmpc	7/8 16:27:15	*TCPDone	0	Client 10.0.0.2:59362 Server 4.26.67.112:80 Client sent 16270 bytes (25 pkts) Server sent 1813
0	gmpc	7/8 16:27:15	*TCPDone	0	Client 10.0.0.2:59364 Server 173.194.33.153:80 Client sent 18697 bytes (34 pkts) Server sent 3
0	gmpc	7/8 16:27:15	*TCPDone	0	Client 10.0.0.2:59365 Server 173.194.33.153:80 Client sent 21120 bytes (41 pkts) Server sent 4
0	gmpc	7/8 16:27:15	*TCPDone	0	Client 10.0.0.2:59366 Server 173.194.33.154:80 Client sent 21208 bytes (31 pkts) Server sent 3
0	gmpc	7/8 16:27:15	*TCPDone	0	Client 10.0.0.2:59367 Server 173.194.33.154:80 Client sent 20061 bytes (28 pkts) Server sent 1
0	gmpc	7/8 16:27:15	*TCPDone	0	Client 10.0.0.2:59368 Server 173.194.33.153:443 Client sent 23770 bytes (42 pkts) Server sent
0	gmpc	7/8 16:27:15	*TCPDone	0	Client 10.0.0.2:59369 Server 173.194.33.153:443 Client sent 22706 bytes (42 pkts) Server sent
0	gmpc	7/8 16:27:15	*TCPDone	0	Client 10.0.0.2:59371 Server 216.39.55.12:80 Client sent 21165 bytes (31 pkts) Server sent 368
0	gmpc	7/8 16:27:15	*TCPDone	0	Client 10.0.0.2:59370 Server 216.39.55.12:80 Client sent 21165 bytes (31 pkts) Server sent 368

Settings	
IP address	192.168.3.220
Port	33333
CI mode	P
CC mode	N
File type	N
File name	glen
F Allocate	20
tcp.com's	1
UDP	0

Status  
Setting conn thread 2 affinity to CPU 4  
Detected IAS Version 2  
Detected 678 Version 2, Supplement B  
End of input stream