

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF TEXAS
MARSHALL DIVISION

ALACRITECH, INC., Plaintiff, v. CENTURYLINK COMMUNICATIONS LLC, et al. Defendants.	Case No. 2:16-cv-693-RWS LEAD CASE JURY TRIAL DEMANDED
ALACRITECH, INC., Plaintiff, v. WINSTRON CORPORATION, et al., Defendants.	Case No. 2:16-cv-692-RWS JURY TRIAL DEMANDED MEMBER CASE
ALACRITECH, INC., Plaintiff, v. DELL INC., Defendant.	Case No. 2:16-cv-695-RWS JURY TRIAL DEMANDED MEMBER CASE

(APPENDIX A)
REPORT OF ALACRITECH'S EXPERT
DR. KEVIN C. ALMEROOTH
CONCERNING INTEL'S INFRINGEMENT

RESTRICTED - ATTORNEYS' EYES ONLY - INTEL ADDENDUM/RESTRICTED
CONFIDENTIAL - SOURCE CODE

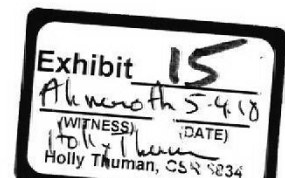


TABLE OF CONTENTS

I. INTEL’S RSC PRODUCTS INFRINGE THE ALACRITECH PATENTS..... 1

 A. Background on RSC 1

 B. Intel’s Accused RSC Product Families..... 5

 C. Each of Intel’s RSC Product Families Infringe Each of Alacritech’s Asserted
 “Receive Side” Claims..... 9

 1. Intel Infringes Claims 1 and 22 of the ‘205 Patent 9

 a. Direct Infringement..... 9

 b. Indirect Infringement 23

 2. Intel Infringes Claims 1, 2, 3, and 4 of the ‘036 Patent 25

 a. Direct Infringement..... 25

 b. Indirect Infringement 35

 3. Intel Infringes Claim 1 of the ‘241 Patent 37

 a. Direct Infringement..... 37

 b. Indirect Infringement 46

 4. Intel Infringes Claims 32 and 41 of the ‘880 Patent 48

 a. Direct Infringement..... 48

 b. Indirect Infringement 67

 5. Intel Infringes Claims 17 and 22 of the ‘948 Patent 69

 a. Direct Infringement..... 69

 b. Indirect Infringement 84

 D. Intel Had Pre-suit Knowledge of the Patents-In-Suit 87

 E. Response to Intel’s Disclosed Theories of Noninfringement 88

II. INTEL’S LSO PRODUCTS INFRINGE THE ALACRITECH PATENTS..... 93

 A. Background on LSO 93

B.	Intel’s Accused LSO Product Families.....	95
C.	Each of Intel’s LSO Product Families Infringe Each of Alacritech’s Asserted “Send Side” Claims.....	107
1.	Intel Infringes Claims 9 and 12 of the ‘241 Patent	108
a.	Direct Infringement.....	108
b.	Indirect Infringement	147
2.	Intel Infringes Claims 1, 15, and 17 of the ‘072 Patent	151
a.	Direct Infringement.....	151
b.	Indirect Infringement	221
D.	Intel Had Pre-suit Knowledge of the Patents-In-Suit	224
E.	Response to Intel’s Disclosed Theories of Noninfringement	226
III.	ABSENCE OF ACCEPTABLE NON-INFRINGEMENT SUBSTITUTES	230
A.	There Are No Acceptable Alternatives to Performing the Functionality in the RSC Claims.....	230
B.	There Are No Acceptable Alternatives to Performing the Functionality in the LSO Claims.....	239

I. INTEL’S RSC PRODUCTS INFRINGE THE ALACRITECH PATENTS

A. Background on RSC

1. As I discuss in the Background of Networking Technology section in the main report, network processing typically progresses through a series of layers. When receiving data from a network, those layers generally require stripping various headers off the packets and checking for the various error conditions that can arise. As discussed above, these repeated verification and header removal steps are traditionally performed by the CPU, which (for large receives) can eat up a lot of the processing power of the CPU.

2. “RSC” is short for “Receive Segment Coalescing” or “Receive Side Coalescing.” “RSC is a stateless offload technology that helps reduce CPU utilization for network processing on the receive side by offloading tasks from the CPU to an RSC-capable network adapter.” (Receive Segment Coalescing, BATES ALA00009425-26 (“Microsoft RSC”).) “RSC enables an RSC-capable network interface card to do the following:

- Parse multiple TCP/IP packets and strip the headers from subsequent packets while preserving the payload of each packet.
- Join the combined payloads of the multiple packets into one packet.
- Send the single packet, which contains the payload of multiple packets, to the network stack for subsequent delivery to applications.”

(*Id.*) In other words, RSC allows the network interface card to process and remove the TCP and IP layers from incoming packets, combine the data or “payload” for those packets into one large logical packet, then send that packet—which contains the data from multiple packets—to the host computer.

3. Intel’s documents confirm that “RSC coalesces incoming TCP/IP packets into larger receive segments.” (BATES 88800DOC031036 – 32447 (“Niantic Datasheet”) at §

7.11.2 Flow Identification and RSC Context Matching

TCP/IP packet’s flow is identified by its four tuples: Source / Destination IP addresses and Source / Destination TCP port numbers. These tuples are compared against the *Flow Identification* fields stored in the active RSC contexts (listed in Table 7-82). Comparison is done in two phases:

- Hash Compare — Hardware computes a hash value of the four tuples for each flow. The hash value is stored in the RSC context table. It is used for silicon optimization of the compare logic. The hash value of the incoming packet is compared against the hash values of all RSC contexts. No match between the two hash values means that there is no valid context of the same flow.
- Perfect Match — Hardware checks the four tuples of the RSC context that passed the first step with the received frame.
 - A match between the two means that an active RSC context is found.
 - Mismatch between the two indicates a hash collision, which causes a completion of the collided RSC.
- In any case of context mismatch, a new context might be opened as described in Section 7.11.3.
- If the packet’s flow matches an active RSC context then the packet might be appended to the existing RSC as described in Section 7.11.4.

(Niantic Datasheet at § 7.11.2; *see also* Sageville Datasheet at § 7.10.2; Twinville Datasheet at § 7.11.2; Broadwell DE Datasheet at § 7.9.2; Denverton Datasheet at § 5.9.2; Louzon Dep. Tr. 198:4 through 200:19; *id.* 217:15-25; Sarangam Dep. Tr. 239:12 through 240:23.)

61. Claim 32[c]: “generating a flow key from said source identifier and said destination identifier to identify a communication flow comprising said packet, wherein said flow key includes a TCP connection for the communication flow and a first hop medium access control (MAC) layer address” After extracting the source and destination TCP ports and the source and destination IP addresses, the accused RSC products generate a hash value based on those four tuples. That hash value is then used to identify an active RSC context, and is thus a flow key or “context identifier” as construed by the Court:

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts



Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research



With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips



Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS

Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS

Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS

Sync your system to PACER to automate legal marketing.