NAME
radump — tcpdump processing of the user data buffers from an argus(8) data file/stream.

SYNOPSIS
radump -r argus-file [raoptions] [-- filter-expression]

DESCRIPTION
Radump reads argus data from an argus data stream or file, and prints out tcpdump style decoding of the user data buffers.

OPTIONS
Radump, like all ra based clients, supports a number of ra options including filtering of input argus records through a terminating filter expression. See ra(1) for a complete description of ra options.

EXAMPLE INVOCATION
This example dumps the user capture buffers of arp traffic seen in the file. When there is no user buffer, or if the decoder can’t decode it, the length will 0.

```bash
% radump -r argus.file -s suser:64 duser:64 -N 5 - arp
srcUdata dstUdata
s[38]="who-has 192.168.0.66 tell 192.168.0.68" d[36]="192.168.0.68 is-at c8:2a:14:58:7a:55"
s[37]="who-has 192.168.0.1 tell 192.168.0.68" d[36]="192.168.0.68 is-at 80:71:1f:3c:cc:03:88"
s[36]="who-has 192.168.0.1 tell 192.168.0.78" d[0]="
s[38]="who-has 192.168.0.34 tell 192.168.0.66" d[0]="
```

This example decodes the user capture buffers of DNS traffic seen in the file.

```bash
% radump -s stime pkts suser:64 duser:64 -r ~/argus/data/argus*00.out.gz - port domain
StartTime TotPkts srcUdata dstUdata
17:48:36.776501 2 s[40]="51781+ [] A? www.surveymonkey.com. (38)" d[31]="51781 1/3/0 A 75.98.93.51 (64)"
```

This example decodes the user capture buffers of HTTP traffic seen in the file.

```bash
radump -s stime proto dport pkts suser:32 duser:32 -r ~/argus/data/argus*00.out.gz - port http
StartTime Proto Dport TotPkts srcUdata dstUdata
17:48:36.632662 tcp http 24 s[32]="/GET /argus/ HTTP/1.1...H0" d[32]="HTTP/1.1 200 OK..Date: M"
```

COPYRIGHT
Copyright (c) 2000-2014 QoSient. All rights reserved.

AUTHORS
Carter Bullard (carter@qosient.com).

SEE ALSO
ra(1), rac(5), argus(8)