Network Capture Prioritization

When planning a network capture, consider the following order of preference to ensure the highest-fidelity evidence acquisition:

- **Network tap at link speed**
- **Port mirror (SPAN Port) on switch**
- **Network tap at less than link speed**

Remember that the interception of other individuals' data is considered an invasion of privacy (or is flat out illegal) in many countries. Check before you capture – involve the legal team early!

As with any evidence, safeguard the network captures carefully, as it could contain sensitive information such as PII, PCI, HIPAA, or other regulated/privileged data.

Correlating Evidence Sources

Obtain a network diagram so you know what is located where both physically and logically.

DHCP and DNS logs often contain helpful evidence that can establish a better understanding of other evidence. For example, knowing the hostname a client system looked up immediately before establishing an SSL connection can be invaluable.

- **DNS query logs for domains looked up from within the environment**
- **DHCP lease logs map MAC addresses to IPs**

Things to Remember

If you have prepared the environment ahead of an incident, the evidence will be there and waiting for collection. If you rush, you might destroy the evidence or otherwise negatively affect its credibility.

Don't rush or panic!

Typical tcpdump Capture Options

Identify available capture interfaces:

```
$ sudo tcpdump -D
```

Prevent DNS and service name lookups:

```
$ sudo tcpdump -nn
```

Capture on interface "eth0", write to file "`output.pcap`"

```
$ sudo tcpdump -nn -i eth0 -w output.pcap
```

Capture only first 56 bytes of each frame – enough to cover the IP header and typical TCP header. (a.k.a. "snaplen of 56".)

```
$ sudo tcpdump -nn -i eth0 \
  -w output.pcap -s 56
```

Attempt to capture the entire contents of each packet (a.k.a "snaplen zero".)

```
$ sudo tcpdump -nn -i eth0 \
  -w output.pcap -s 0
```

Use a filesize-based "ring buffer" of 10 files, 100MB each. Overwrite oldest file after 10 files have been created. Second and later output files will have a digit appended to the filename (e.g. "`output.pcap0`", "`output.pcap1`", etc.).

```
$ sudo tcpdump -nn -i eth0 \
  -w output.pcap -C 100 -W 10
```

Use a time-based ring buffer with 14 files, which contain 12 hours (43,200 seconds). Overwrite oldest file after 10 files have been created. Filenames will contain appended digits as described above.

```
$ sudo tcpdump -nn -i eth0 \
  -w output.pcap -G 43200 -W 14
```

NOTE: Not all tcpdump versions and distributions provide all options. Verify capture commands before running them!

Evidence Collection Cheat Sheet

POCKET REFERENCE GUIDE

SANS Institute
http://computer-forensics.sans.org

by Steve Armstrong, Phil Hagen

Purpose

This sheet covers the various locations where evidence to assist in an investigation may be located.

Time

Identity the timeserver, time zone & skew: For Windows 2000 and 2003 systems:

```
C:\> net time
```

From Windows 2008, 7 and 8

```
C:\> w32tm /query / source
```

If the service is not running, pull from the registry:

```
C:\> w32tm /dumpreg
```

To identify the system's time zone:

```
C:\> w32tm /tz
```

In Linux, OS X, and other Unix-like systems display UTC with the following command:

```
$ date -u
```

Be careful if you are root – this command can also reset the system time!

Exporting NetFlow Data

`fprobe` can be used to export NetFlow data from a Linux/Unix-like host to a collector (specified by IP)

```
$ fprobe -i eth0 -f 'ip' 192.168.1.15:9995
```

Capturing Exported NetFlow Data

`nfcapd` is a NetFlow capture daemon.

```
$ nfcapd -p 9995 -4 -w -D \
  -n <host_id>,<exporter_IP>,/path/to/dir
```

Specify the storage directory naming convention with the `-S` switch – see the man page for available formats.

nfdump Input and Time Slicing

`nfdump` can read from one or more files, or a directory tree full of files.

```
-r <filename>
-R <list of files or directories>
```

To limit a query to a specific time frame, use the `-t` switch with times specified as "`YYYY/MM/dd.hh:mm:ss`". Lower-order time components may be omitted (e.g. "`YY/MM/dd`" for day-level granularity).

```
-t '<starttime>[-<endtime>]'
```

nfdump Output Formats

There are several pre-defined output formats plus a custom formatting option. Use the `-o` switch to specify.

`-o line`	(default) One flow per line
`-o long`	One line per flow with TCP flags and TOS values
`-o extended`	One line per flow with TCP flags, TOS, packets/sec, bits/sec, and bits/packet values
`-o csv`	All values displayed in CSV

nfdump Output Formats, Cont.

A number of format strings can be used with `nfdump` to change how the output is displayed

```
$ nfdump -r <in file> -o "fmt:<fmt str>"
```

`%ts`	Start Time	**`%in`**	Input Int Num
`%te`	End Time	**`%out`**	Output Int num
`%td`	Duration	**`%pkt`**	Packets
`%pr`	Protocol	**`%byt`**	Bytes
`%sa`	Src Address	**`%fl`**	Flows
`%da`	Dst Address	**`%pkt`**	Packets
`%sap`	Src Address:Port	**`%flg`**	TCP Flags
`%dap`	Dst Address:Port	**`%tos`**	Type of service
`%sp`	Src Port	**`%bps`**	bits/second
`%dp`	Dst Port	**`%pps`**	packets/second
`%sas`	Src AS	**`%bpp`**	bits/packet
`%das`	Dst AS		

Use this option to generate custom CSV, which can be imported to other tools for processing or visualization.

```
$ nfdump -r <in file(s)> \
  -o "fmt:%pkt,%sa,%da" > netflow.csv
```

Aggregate output records:

- **`-a`** Aggregate by the standard NetFlow 5-tuple (proto, srcip, dstip, srcport, and dstport)
- **`-b`** Automatic bidirectional aggregation
- **`-B`** Semi-intelligent bidirectional aggregation (tries to identify client and server based on port >1024)
- **`-A`** Custom aggregation fields – see man page

View the "topN" talkers to identify the noisiest IPs by flow count. (See the man page for additional statistic calculations and ordering options to the `-s` switch.)

```
$ nfdump -r <in file(s)> -s ip/flows -n 10
```

Display a limited number of records with the `-c` switch.

```
$ nfdump -r <in file(s)> -c <record_limit>
```


Wireless

For Wireless networks investigations, supplement standard log data with Wireless DHCP Servers logs, Wireless IDS Logs, Access Point Logs, and Wireless LAN Controller logs, and client logs:

In Apple OS X:

- **In the Console application, search all messages for 'airport'**

In Windows 7 and later, use Event Viewer to obtain the **Operational** log from:
Applications and Service Logs -> Microsoft -> Windows -> WLAN-AutoConfig

In Linux and other Unix-like OSes examine the files in the **`/var/log/`** directory.

Switches

For localized incidents, switching equipment can be incredibly revealing. Focus on the following:

- **Switch CAM Tables to map MACs to Ports**
- **Switch OS version and patch levels**
- **Switch live port status**
- **Switch port configuration (VLAN, SPAN/Port mirroring, etc.)**
- **Switch ACLs**

This evidence can quickly lead the investigator to the physical network segment or device responsible for anomalous or suspicious activity.