



# 'From Data Collection To Action' Achieving Rapid Identification of Cyber Threats and Perpetrators

**Joel Ebrahimi**  
**Solutions Architect**  
**Bivio Networks, Inc.**

# Data Retention Defined

---

- /// Key piece of comprehensive Cyber Security strategy
- /// Investigative tool: provides ability to look back in time
- /// Complements and enhances existing tools
  - Lawful Interception
  - Packet capture/re-play



# A Transforming Network

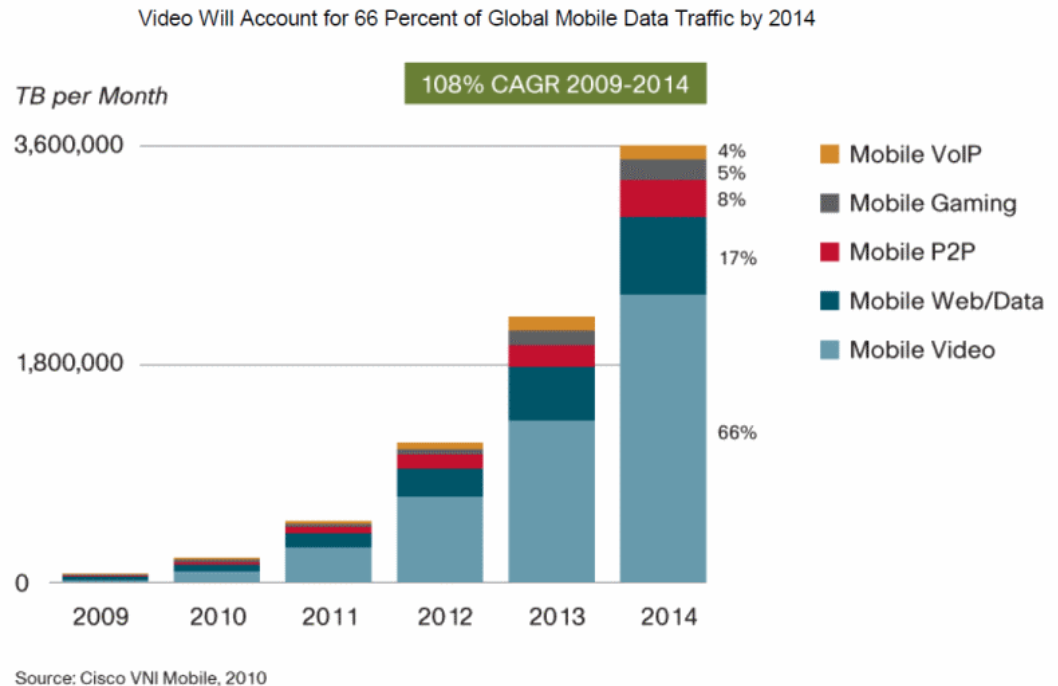
---

- /// Explosion in usage, applications, devices, protocols
- /// Basic networking problems remain
  - Security
  - Information assurance
  - Cyber defense
  - Awareness
  - Control
- /// Network role transition from connectivity to policy



# Exponential Growth in Mobile Devices

- Mobile Internet use is exploding
  - Information exchange
  - Entertainment
  - Social networking
  - Business productivity

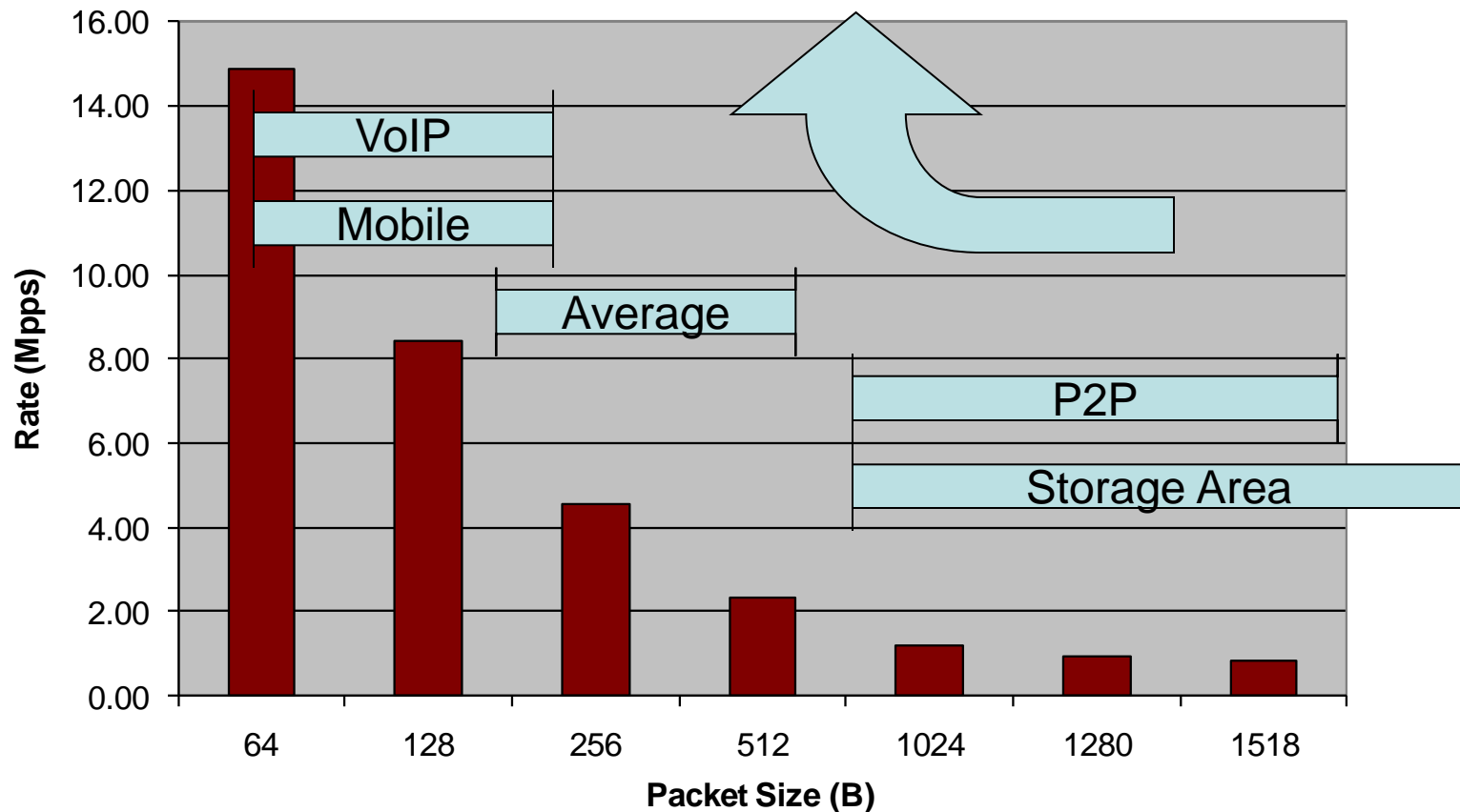


Mobile access leads to new challenges...

# Increasing Throughput

Performance of DPI functions significantly harder to maintain at 10Gbps speeds.

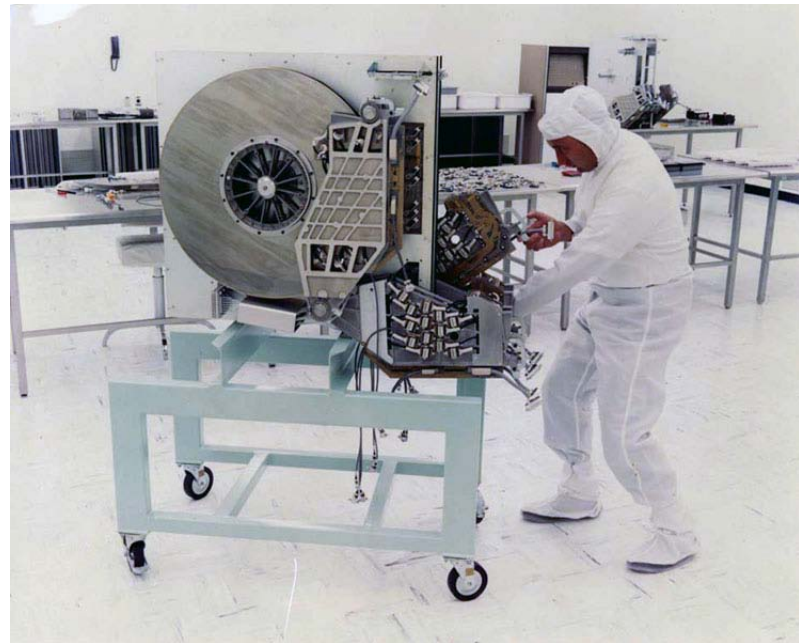
- Network Applications drive overall network impact



# Packet Capture Madness!

---

- /// 1 Min – 75 GB
- /// 1 Hour – 4500 GB
- /// 1 Day – 100.5 TB
- /// 1 Month 3000 TB



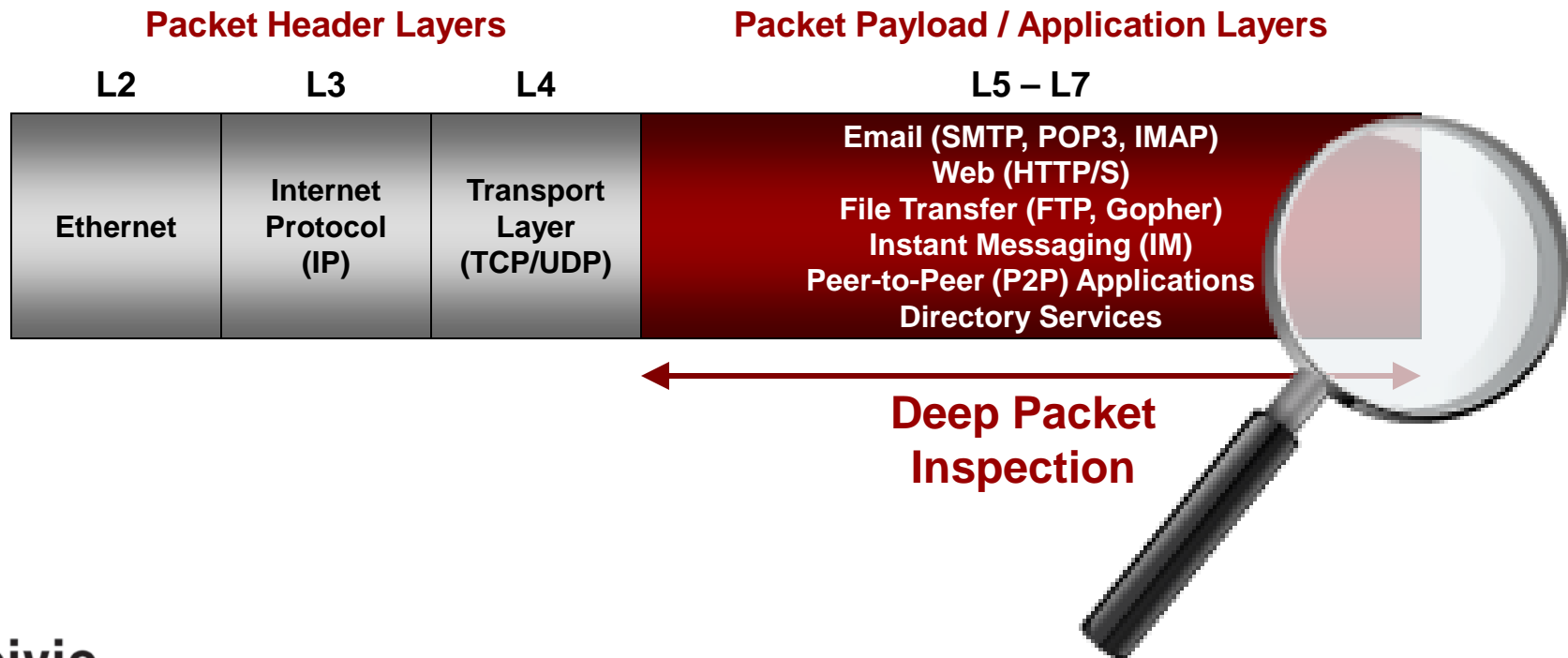
# Many Required Technologies

---

- /// Fast capture hardware/DPI technology
- /// Meta Data
- /// Storage Farm
- /// The ability to retrieve in a reasonable amount of time

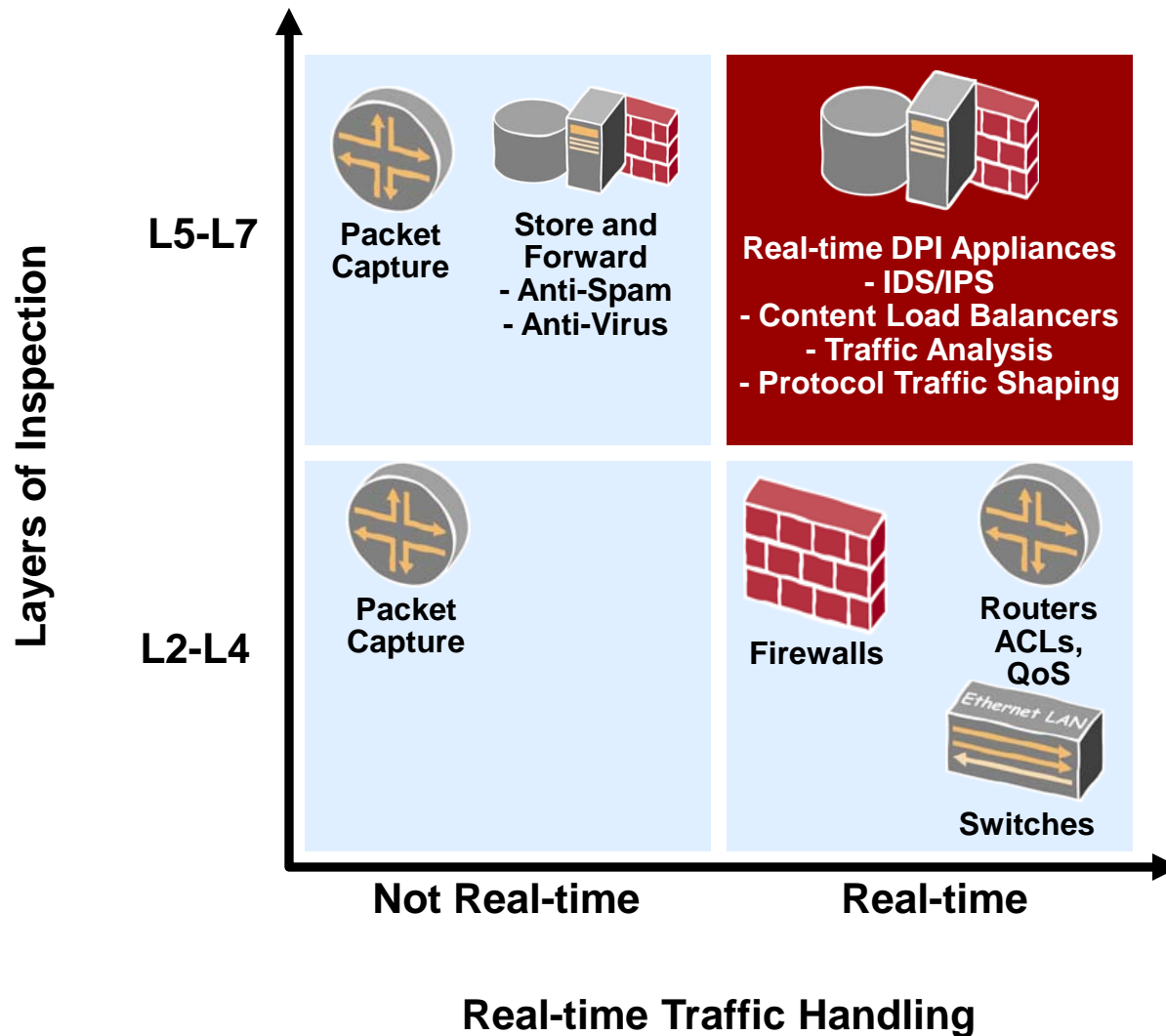
# What is Deep Packet Inspection?

**Deep Packet Inspection (DPI) is a form of filtering that examines (inspects) both the payload and the header of a packet as it passes an inspection point.**





# DPI Hardware Implementations



# Meta Data

The image shows a Wireshark capture of an HTTP transaction. The packet list pane shows a sequence of packets: SYN, ACK, ACK, GET, and another ACK. The selected packet (No. 6) is an ACK from 10.0.1.101 to 10.0.2.102. The packet details pane shows the Ethernet II, Internet Protocol, and Transmission Control Protocol (TCP) layers. The TCP layer shows the source port as 1091 and the destination port as 80. The Hypertext Transfer Protocol layer is expanded to show the raw data.

No.	Time	Source	Destination	Protocol	Info
1	0.000000	10.0.2.102	10.0.1.101	TCP	ff-sm > http [SYN] Seq=0 win=65535 Len=0 MSS=1460 SACK_PERM=1
2	0.000675	10.0.1.101	10.0.2.102	TCP	http > ff-sm [SYN, ACK] Seq=0 Ack=1 win=16384 Len=0 MSS=1460 SACK_PERM=1
3	0.002908	10.0.2.102	10.0.1.101	TCP	ff-sm > http [ACK] Seq=1 Ack=1 win=65535 Len=0
4	0.005269	10.0.2.102	10.0.1.101	HTTP	GET /Security/Anonymous/ HTTP/1.1
5	0.009399	10.0.1.101	10.0.2.102	HTTP	HTTP/1.1 200 OK (text/html)
6	0.173974	10.0.2.102	10.0.1.101	TCP	ff-sm > http [ACK] Seq=305 Ack=402 win=65134 Len=0

Frame 5: 455 bytes on wire (3640 bits), 455 bytes captured (3640 bits) on interface 0  
Arrival Time: Feb 11, 2006 14:55:32.211186000 Pacific Standard Time  
Epoch Time: 1139698532.211186000 seconds  
[Time delta from previous captured frame: 0.004130000 seconds]  
[Time delta from previous displayed frame: 0.004130000 seconds]  
[Time since reference or first frame: 0.009399000 seconds]  
Frame Number: 5  
Frame Length: 455 bytes (3640 bits)  
Capture Length: 455 bytes (3640 bits)  
[Frame is marked: False]  
[Frame is ignored: False]  
[Protocols in frame: eth:ip:tcp:http:data-text-lines]  
[Coloring rule Name: HTTP]  
[Coloring rule String: http || tcp.port == 80]  
Ethernet II, Src: Microsoft\_57:ab:2a (00:03:ff:57:ab:2a), Dst: 02:00:4c:4f:4f:50 (02:00:4c:4f:4f:50)  
Internet Protocol, Src: 10.0.1.101 (10.0.1.101), Dst: 10.0.2.102 (10.0.2.102)  
Version: 4  
Header length: 20 bytes  
Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)  
Total length: 441  
Identification: 0x8563 (34147)  
Flags: 0x02 (Don't Fragment)  
Fragment offset: 0  
Time to live: 128  
Protocol: TCP (6)  
Header checksum: 0x5c11 [correct]  
Source: 10.0.1.101 (10.0.1.101)  
Destination: 10.0.2.102 (10.0.2.102)  
Transmission Control Protocol, Src Port: http (80), Dst Port: ff-sm (1091), Seq: 1, Ack: 305, Len: 401  
Hypertext Transfer Protocol  
Line-based text data: text/html

```
0010 01 b9 85 63 40 00 80 06 5c 11 0a 00 01 65 0a 00  ..cB...\\...e..
0020 02 66 00 50 04 43 4f cc 8b 57 09 3e 1a 94 50 18  .f.P.CO..w..P.
0030 fe cf 60 e0 00 00 48 54 54 50 2f 31 2e 31 20 32  .....HT TP/1.1.2
0040 30 30 20 4f 4b 0d 0a 43 6f 6e 74 65 6e 74 2d 4c 00 OK..Content-L
0050 65 6e 67 74 68 3a 20 31 30 37 0d 0a 43 6f 6e 74  ength: 1 07..Cont
0060 65 6e 74 2d 54 79 70 65 3a 20 74 65 78 74 2f 68 ent-type : text/h
0070 74 6d 6c 0d 0a 43 6f 6e 74 65 6e 74 2d 4c 6f 63 tml..Content-Loc
0080 61 74 69 6f 6e 3a 20 68 74 74 70 3a 2f 2f 62 69 ation: h ttp://b1
0090 6c 6e 2e 69 6e 73 2e 63 6f 6d 2f 53 65 63 75 72 11.ins.c om/Secur
00a0 69 74 79 2f 41 6e 6f 6e 79 6d 6f 75 73 2f 69 6e ity/Anon ymous/in
00b0 64 65 78 2e 68 74 6d 0d 0a 4c 61 73 74 2d 4d 6f dex.htm. .Last-Mo
00c0 64 69 66 69 65 64 3a 20 53 61 74 2c 20 31 31 20 dified: Sat, 11
00d0 46 65 62 20 32 30 30 36 20 32 32 3a 34 38 3a 30 Feb 2006 22:48:0
00e0 34 20 47 4d 54 0d 0a 41 63 63 65 70 74 2d 52 61 4 GMT..A ccept-Ra
00f0 6e 67 65 73 3a 20 62 79 74 65 73 0d 0a 45 54 61 nges: by tes..ETA
0100 67 3a 20 22 38 30 34 39 63 66 33 37 35 64 32 66 g: "8049 cf35d2f
0110 63 3e 31 3a 34 30 31 2f 0e 0a 83 65 6f 6e 73 20 c61401" ..Server
0120 3a 20 4d 69 63 72 6f 73 6f 66 74 2d 49 49 53 2f : Micro soft-IIS/
0130 3e 2e 30 0d 0a 44 61 74 65 3a 20 53 61 74 2c 20 6.0..Dat e: Sat,
0140 31 31 20 46 65 62 20 32 30 30 36 20 32 32 3a 35 11 Feb 2 006 22:5
0150 35 31 32 34 20 47 4d 54 0d 0a 0d 0a 0d 0a 0d 0a 524 GMT ..RTD
0160 4c 3e 0d 0a 3c 34 49 54 4c 45 3e 20 55 73 65 72 L>..<!! LE> User
0170 20 61 75 74 68 65 6e 74 69 63 61 74 69 6f 6e 20 authentic ation
0180 3c 2f 54 49 54 4c 45 3e 0d 0a 0d 0a 3c 42 4f 44 </TITLE> ...<BO
0190 69 3e 0d 0a 0d 0a 41 6e 6f 6e 79 6d 6f 75 73 20 Y>...AR otymous
01a0 41 75 74 68 65 6e 74 69 63 61 74 69 6f 6e 2e 0d Authentic ation..
01b0 0a 0d 0a 3c 2f 42 4f 44 59 3e 0d 0a 0d 0a 0d 0a ...</BO D Y>.....
01c0 3c 2f 48 54 4d 4c 3e </HTML>
```

# What is required now?

---

- /// What capabilities / technical features are required by cyber analysts now (in order to have useful investigative information or evidence)?
  - Relationship of IP data flow to a specific person
  - Relationship of domain used to web activity
  - Relationship of time related to specific activities
  - Location of device/person at time of event
  - Secure/protected access, especially in multi-agency environments
  - Scalability of system solution

# Storage

---

- /// Network Attached Storage
- /// Disk Arrays
- /// Store and Forward

# Fast Retrieval

---

- /// Solid State Drives
- /// Properly formatted queries
- /// Indexed Databases

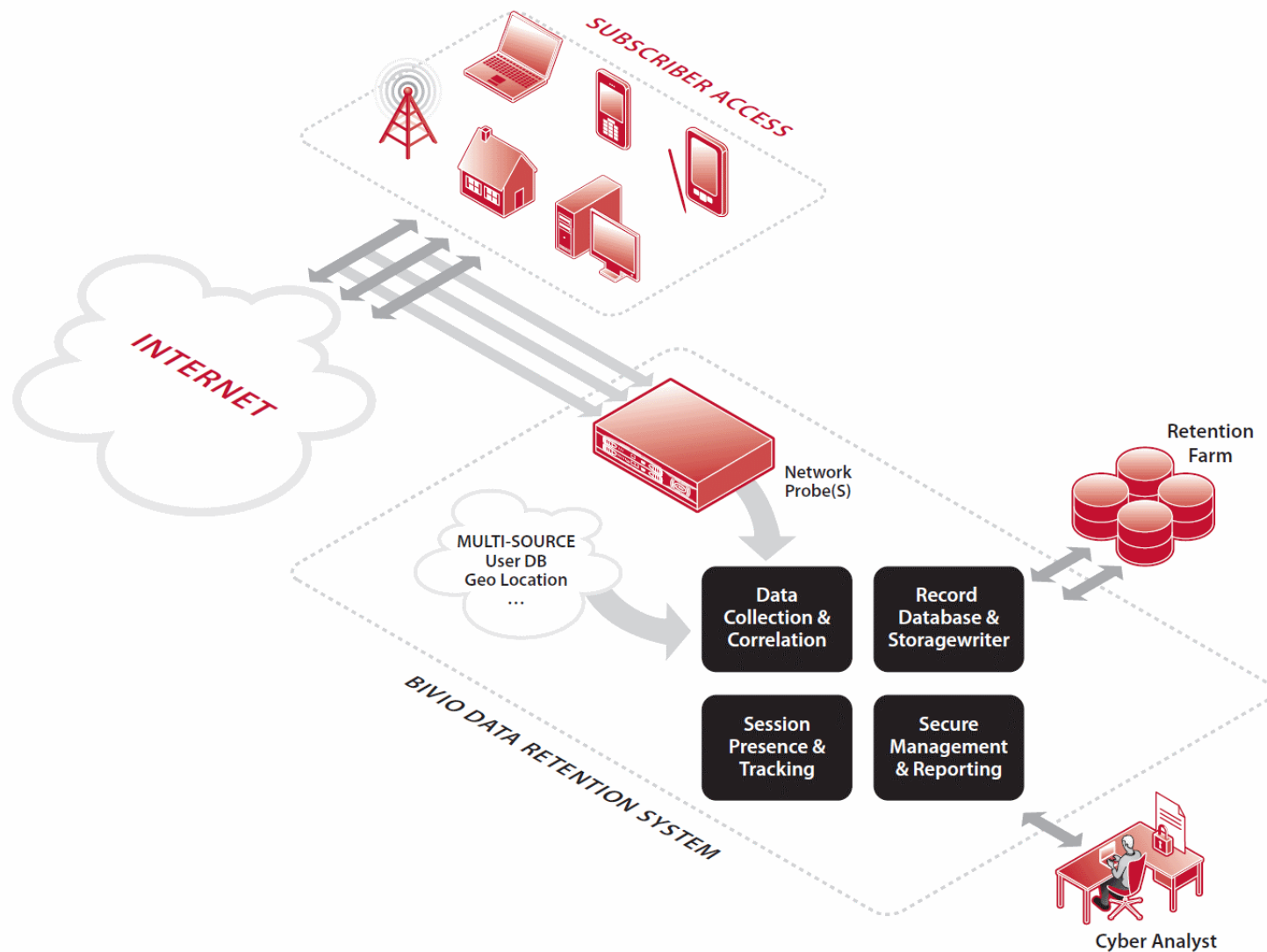
# Data Retention

---

- /// Key piece of comprehensive Cyber Security strategy
- /// Investigative tool: provides ability to look back in time
- /// Complements and enhances existing tools
  - Lawful Interception
  - Packet capture/re-play

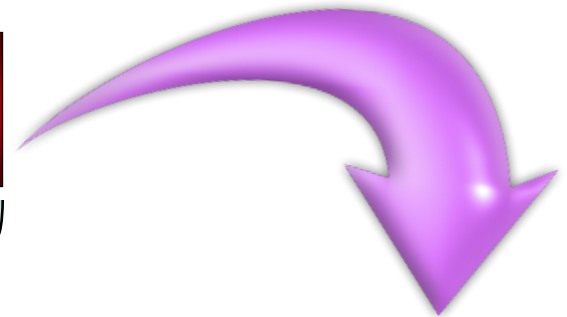
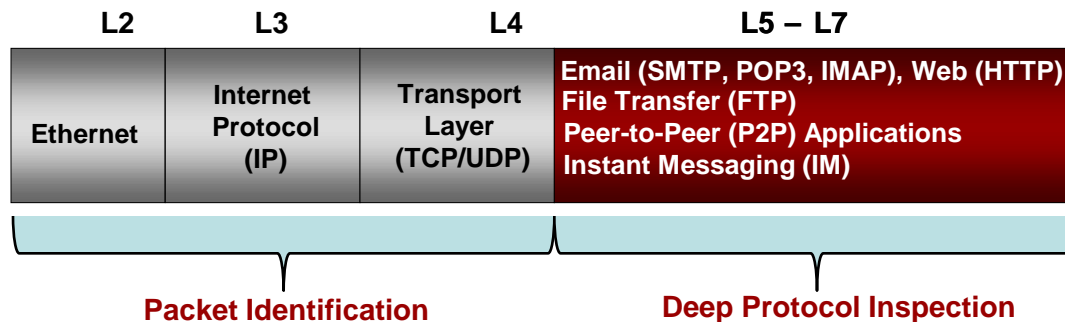


# Network Probe



# Context: Deep Packet Inspection Probing

- /// Far beyond legacy Layer 3/4 flow recording
- /// Far beyond protocol DPI
- /// Extraction of specific protocol or application info
- /// Enables vastly richer data mining and information set
- /// Enables run-time “user” identification through correlation





# Deep Packet Inspection Probing

```
No.    Time    Source      Destination  Protocol Info
167207 0.756202890 10.145.19.66 10.145.19.90  GTP <HTTP> GET /img/2009/11/21/90x90-
alg_image.jpg HTTP/1.1

Frame 167207 (671 bytes on wire, 671 bytes captured)
Ethernet II, Src: Ericsson_ed:81:b0 (00:01:ec:ed:81:b0), Dst: JuniperN_67:5f:f1 (00:23:9c:67:5f:f1)
802.1Q Virtual LAN, PRI: 0, CFI: 0, ID: 202
Internet Protocol, Src: 65.213.148.66 (65.213.148.66), Dst: 65.213.148.6 (65.213.148.6)
User Datagram Protocol, Src Port: blackjack (1025), Dst Port: gtp-user (2152)
GPRS Tunneling Protocol
Internet Protocol, Src: 10.145.19.66 (10.145.19.66), Dst: 10.145.19.90 (10.145.19.90)
Transmission Control Protocol, Src Port: 53585 (53585), Dst Port: http (80), Seq: 1, Ack: 3683, Len: 565
Hypertext Transfer Protocol
GET /img/2009/11/21/90x90-alg_image HTTP/1.1\r\n
[Expert Info (Chat/Sequence): GET /img/2009/11/21/90x90-alg_image.jpg HTTP/1.1\r\n]
[Message: GET /img/2009/11/21/90x90-alg_image.jpg HTTP/1.1\r\n]
[Severity level: Chat]
[Group: Sequence]
Request Method: GET
Request URI: /img/2009/11/21/90x90-alg_image.jpg
Request Version: HTTP/1.1
User-Agent: Mozilla/5.0 (Macintosh; U; Intel Mac OS X 10_5_2; en-us) AppleWebKit/525.18
(KHTML, like Gecko) Version/3.1.1 Safari/525.18\r\n
Referer: http://www.nydailynews.com/real_estate/2010/01/01/2010-01-
01_iconic_nyc_restaurant_tavern_on_the_green_closes_its_doors_friday_after_a_final_.html\r\n
Accept: */*\r\n
Accept-Language: en-us\r\n
Accept-Encoding: gzip, deflate\r\n
Cookie: WT_FPC=id=18.15.2.12-3609171504.30087201:lv=1277848799597:ss=1277848799597\r\n
Connection: keep-alive\r\n
Host: assets.nydailynews.com\r\n
\r\n
```

Deep Packet Inspection



# Correlation Example

A  
P  
P  
L  
I  
C  
A  
T  
I  
O  
N  
S  
I  
P

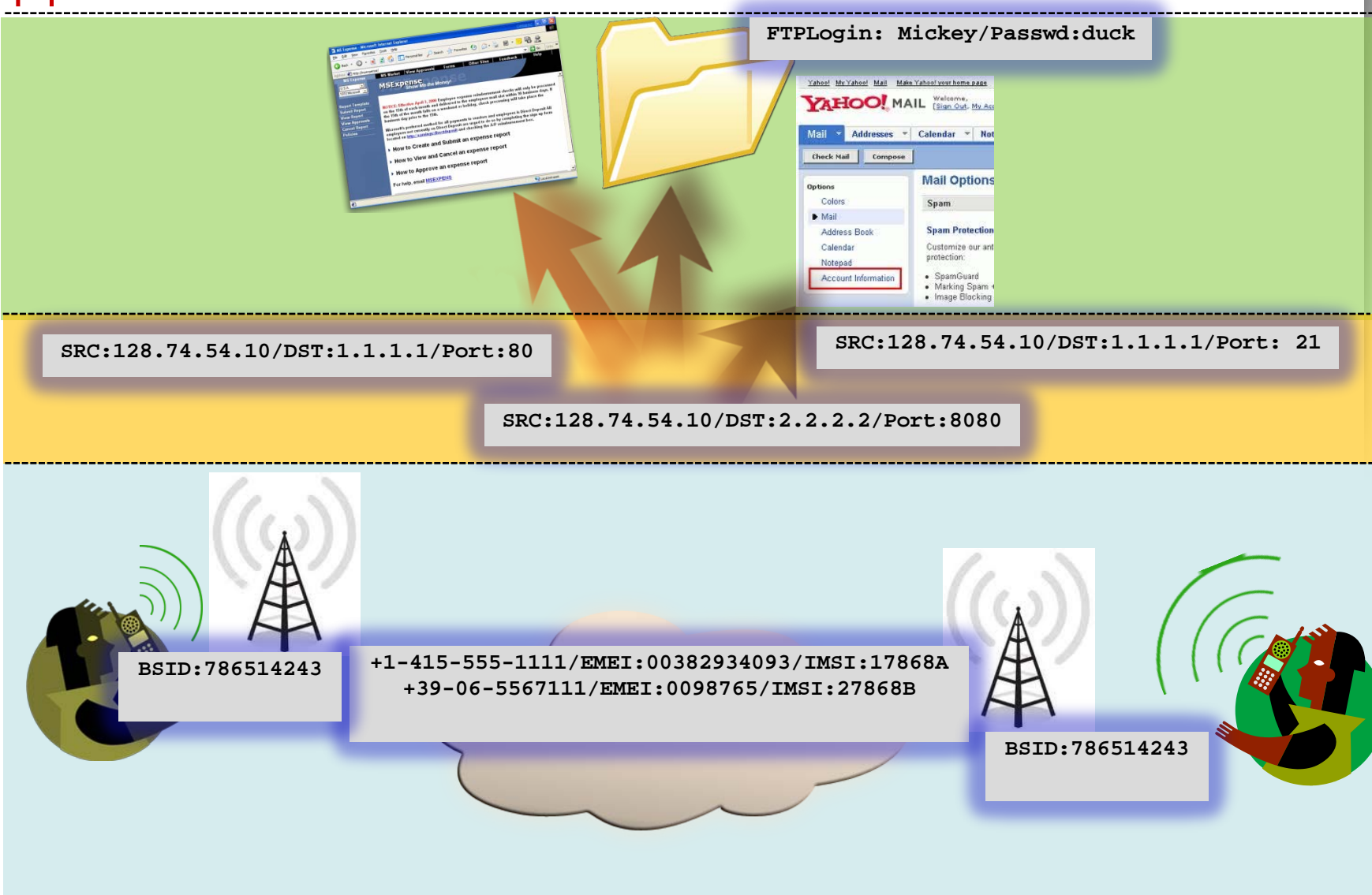


I  
n  
f  
r  
a  
s  
t  
r  
u  
c  
t  
u  
r  
e



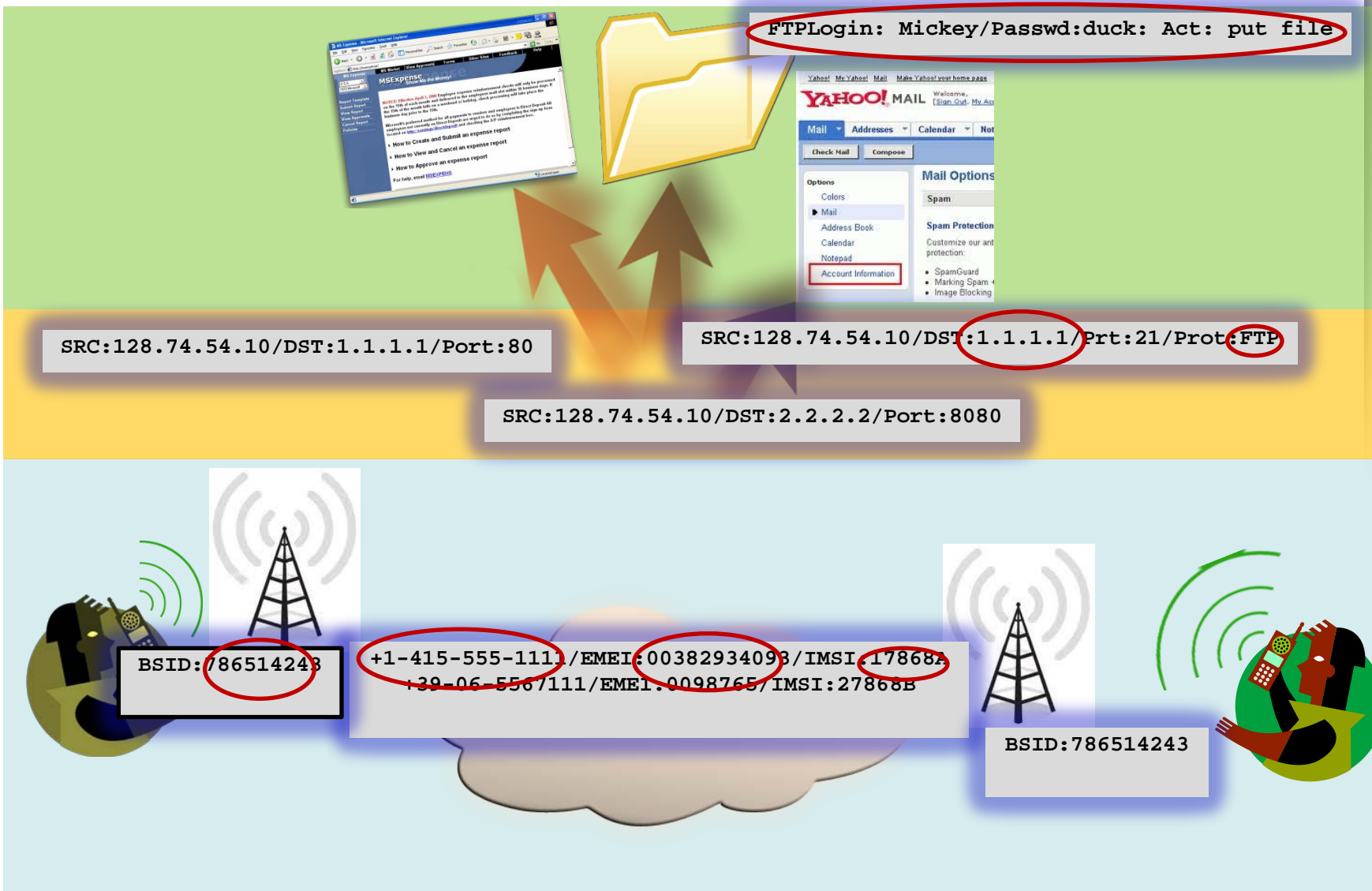
# Correlation Example: Traditional DR approach

A  
p  
p  
l  
i  
c  
a  
t  
i  
o  
n  
s  
  
I  
P  
  
I  
n  
f  
r  
a  
s  
t  
r  
u  
c  
t  
u  
r  
e



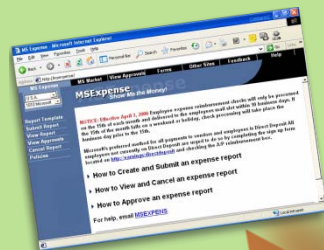
# Bivio Data Retention: Correlation for Context

A  
p  
p  
l  
i  
c  
a  
t  
i  
o  
n  
s  
  
I  
P  
  
I  
n  
f  
r  
a  
s  
t  
r  
u  
c  
t  
u  
r  
e



# Bivio Data Retention: Correlation for Context

A  
p  
p  
l  
i  
c  
a  
t  
i  
o  
n  
s  
I  
P  
I  
n  
f  
r  
a  
s  
t  
r  
u  
c  
t  
u  
r  
e



FTPLogin: Mickey/Passwd:duck: Act: put file



SRC:128.74.54.10/DST:1.1.1.1/Port:80

SRC:128.74.54.10/DST:1.1.1.1/Prt:21/Prot:FTP

SRC:128.74.54.10/DST:2.2.2.2/Port:8080

BSID:786514243

+1-415-555-1111/IMEI:35880801070760/IMSI:17868A  
+39-06-5567111/IMEI:0098765/IMSI:27868B

BSID:786514243

```
RecNo:02A78BH83: +1-415-555-1111[IMEI:35880801070760/IMSI:17868A] frm 786514243
=> FTP {
Session Info: IP:1.1.1.1
Credential: Mickey/duck
Action: put file}
```

# Case Study: Bomb Threat Response

---

- 12.00 pm: *Police noticed a menace message posted on a forum (about a bomb placed in central but unknown location)*
- 12.20 pm: *Secret Services engaged*
- 12.30 pm: *Contacted forum provider to determine the local user credential*
- 12.30 pm: *At the same time, contacted Bivio DRS administrator to retrieve data about sessions created toward the forum site*
- 12.35 pm: *Input query into the system "Which IP addresses accessed the forum site with the specific forum username?"*
- 12.36 pm: *Confirmed the carrier owning the SRC IP*
- 12.36 pm: *Input query into the system "To whom has the IP Address been assigned within the current timeframe?"*
- 12.36 pm: *Input query into the system "Which connection medium has the user used to access the network?"*
- 12.37 pm: *Result: IP -> subscriber ID -> BSID (Wimax) -> CPE Mac address -> user mac address*
- 12.40 pm: *CPE MAC correlated to CPE registration information, including name and address  
User MAC correlated to hardware element, confirming the owner's laptop  
BSID confirmed physical home address covered by the BSS quadrant*
- 14.01 pm: **Suspect caught !**



# Summary

---

- /// Data Retention an essential tool for Cyber Security
- /// Existing solutions focus on “retention” rather than enabling action and response
- /// Next generation DR systems must combine user context, correlation and coverage
- /// DR need to leverage DPI technology, Meta data, and storage and retrieval





Thank You

**Joel Ebrahimi**

**Contact: [jebrahimi@bivio.net](mailto:jebrahimi@bivio.net)**