bivio networks

‘From Data Collection To Action’ Achieving Rapid Identification of Cyber Threats and Perpetrators

Joel Ebrahimi
Solutions Architect
Bivio Networks, Inc.

Data Retention Defined

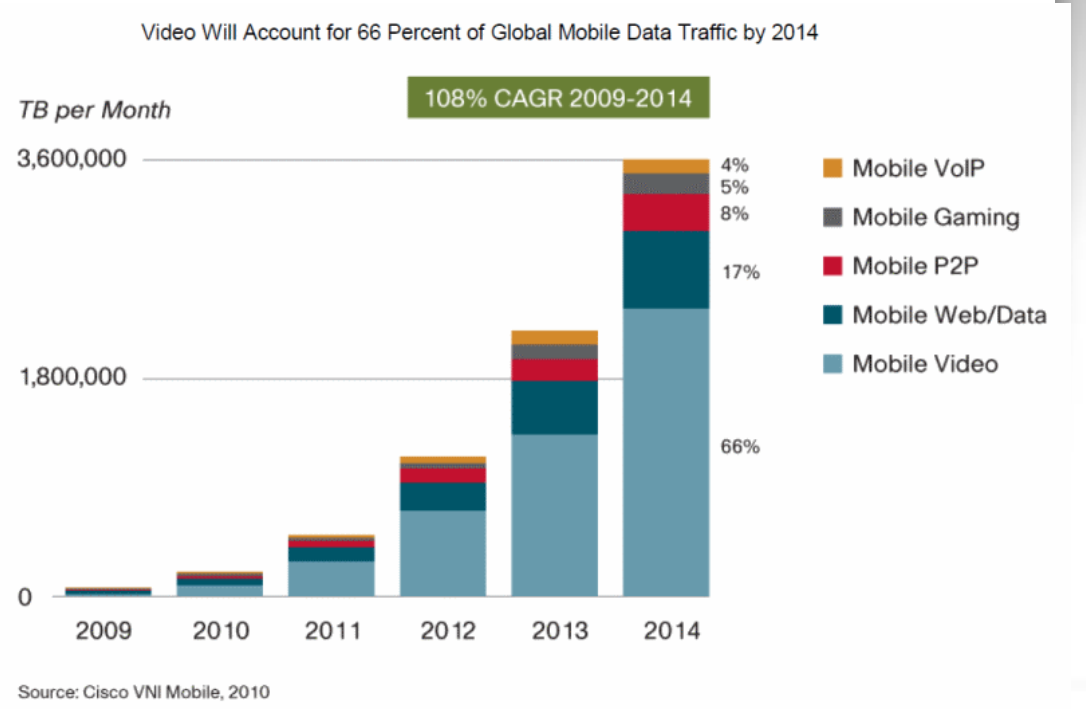
- Key piece of comprehensive Cyber Security strategy
- Investigative tool: provides ability to look back in time
- Complements and enhances existing tools
  - Lawful Interception
  - Packet capture/re-play

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

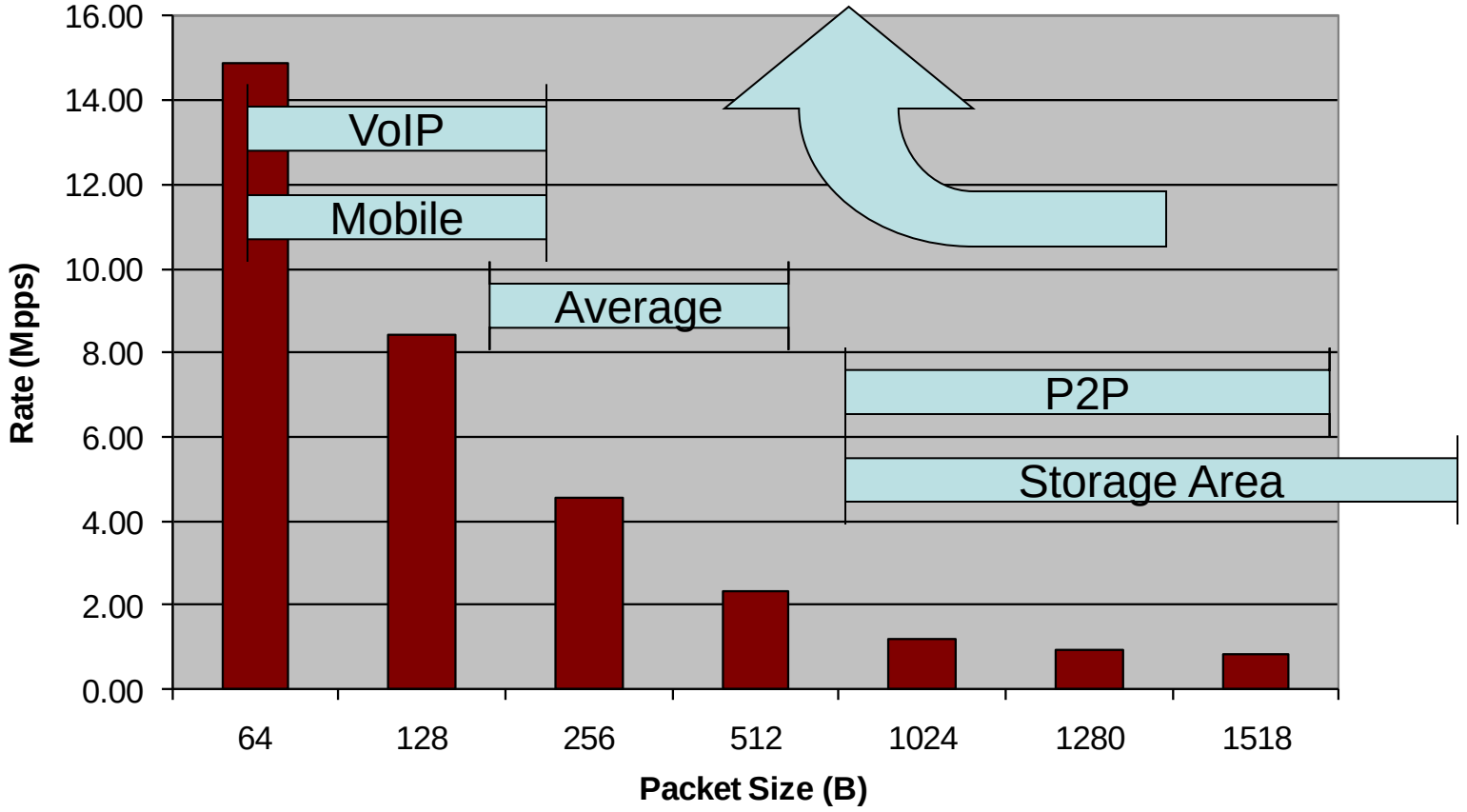


- **All this access leads to new challenges…**

Increasing Throughput

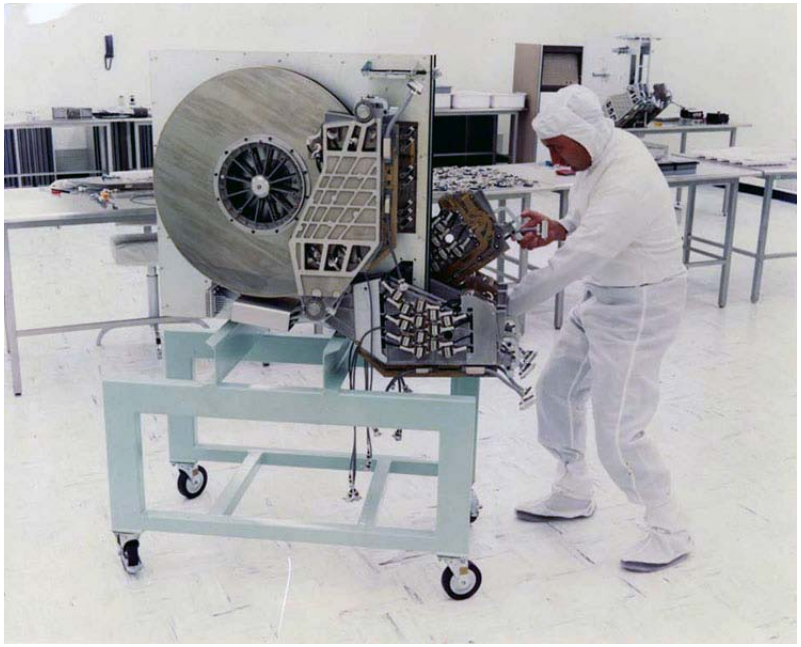
Performance of DPI functions significantly harder to maintain at 10Gbps speeds.

- 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



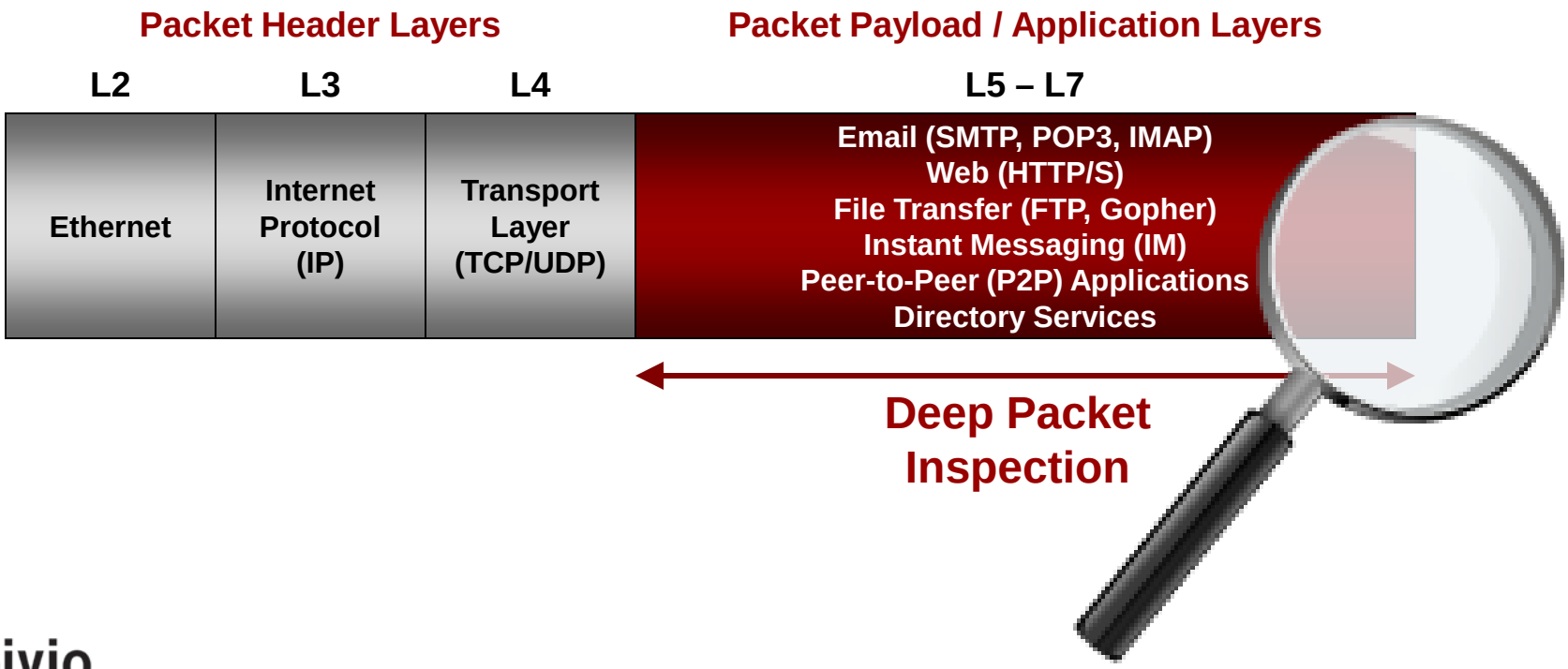
Many Required Technologies

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

bivio networks

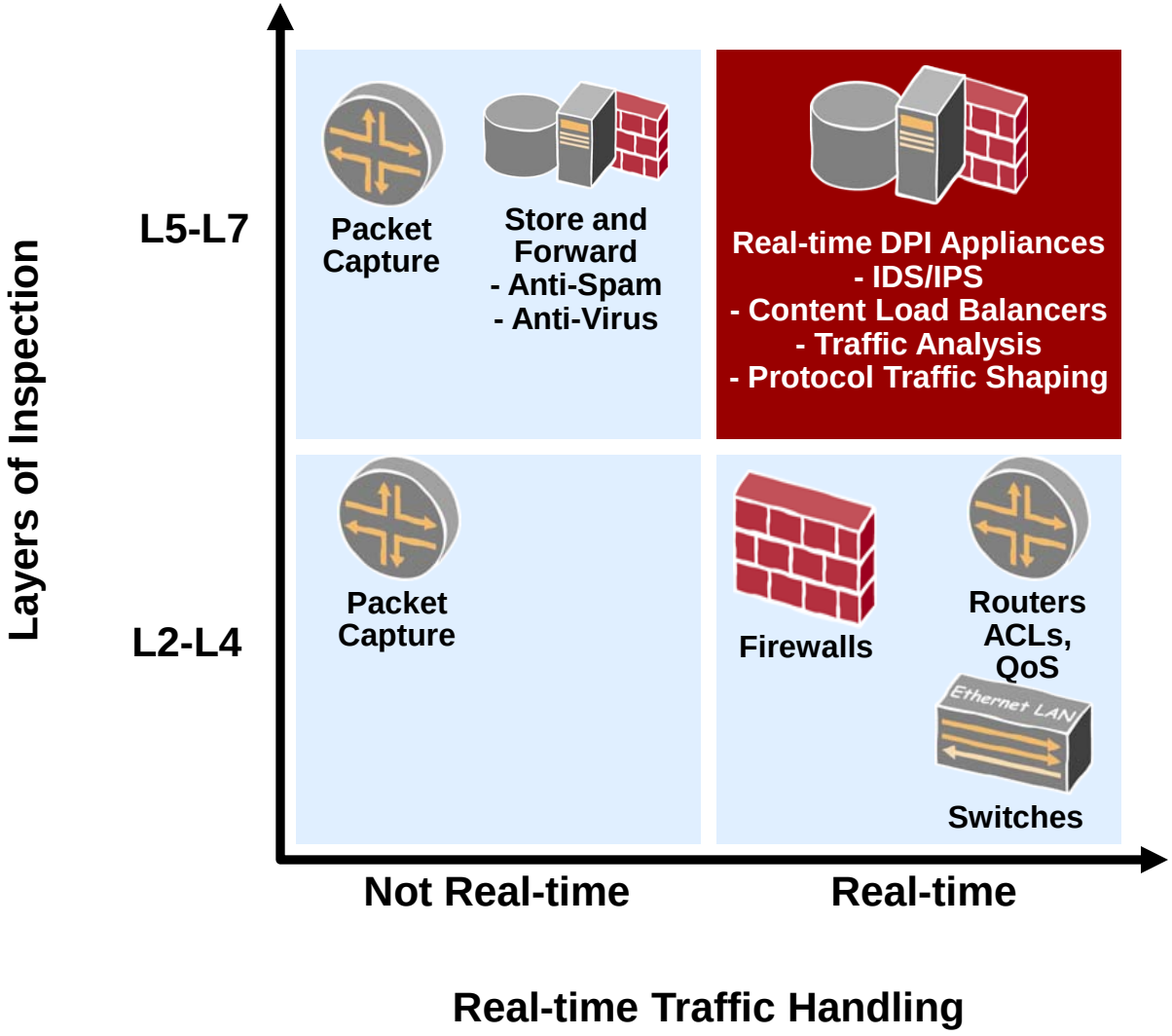
What is Deep Packet Inspection?

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.

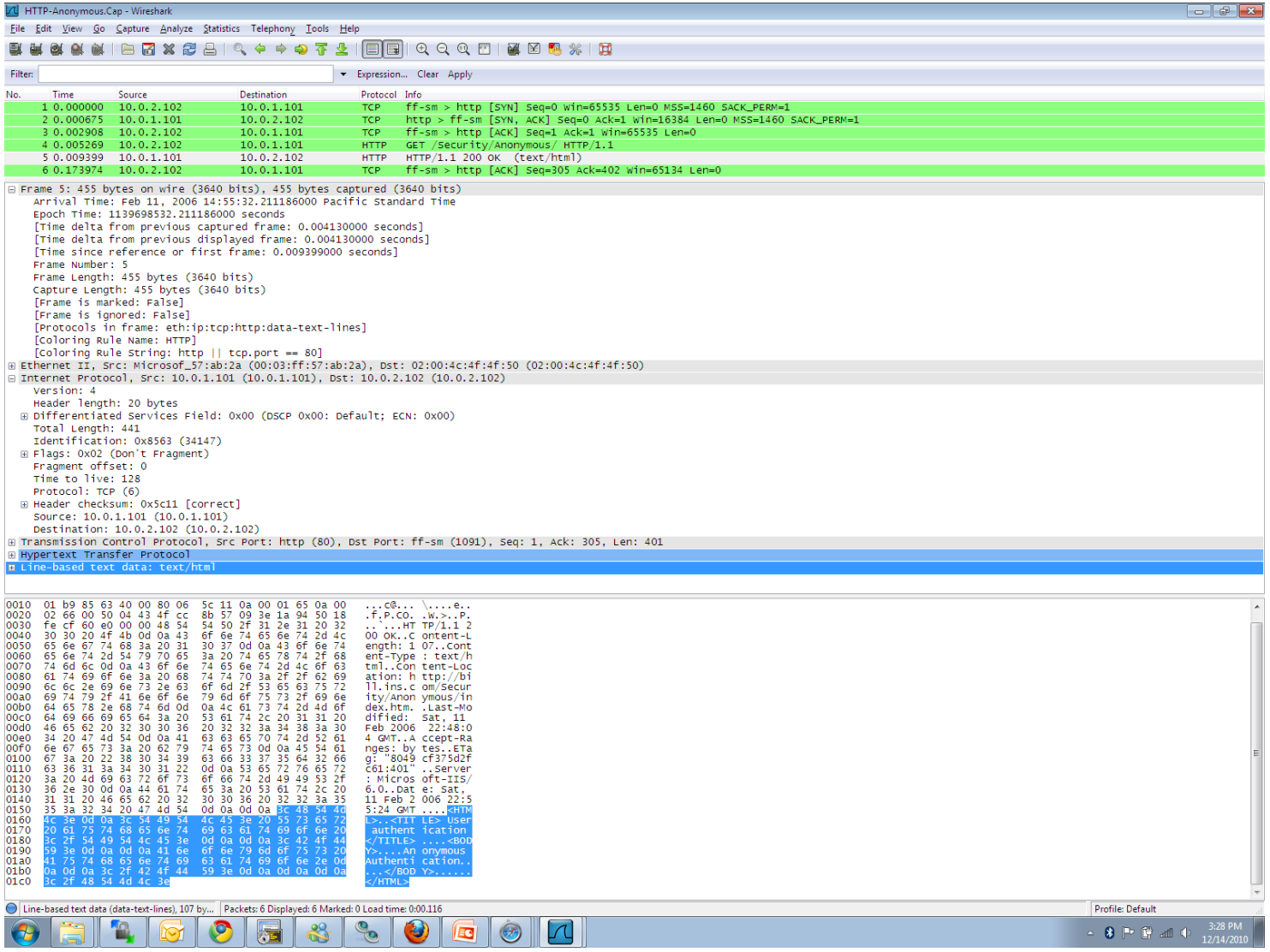


bivio networks

DPI Hardware Implementations



Meta Data



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

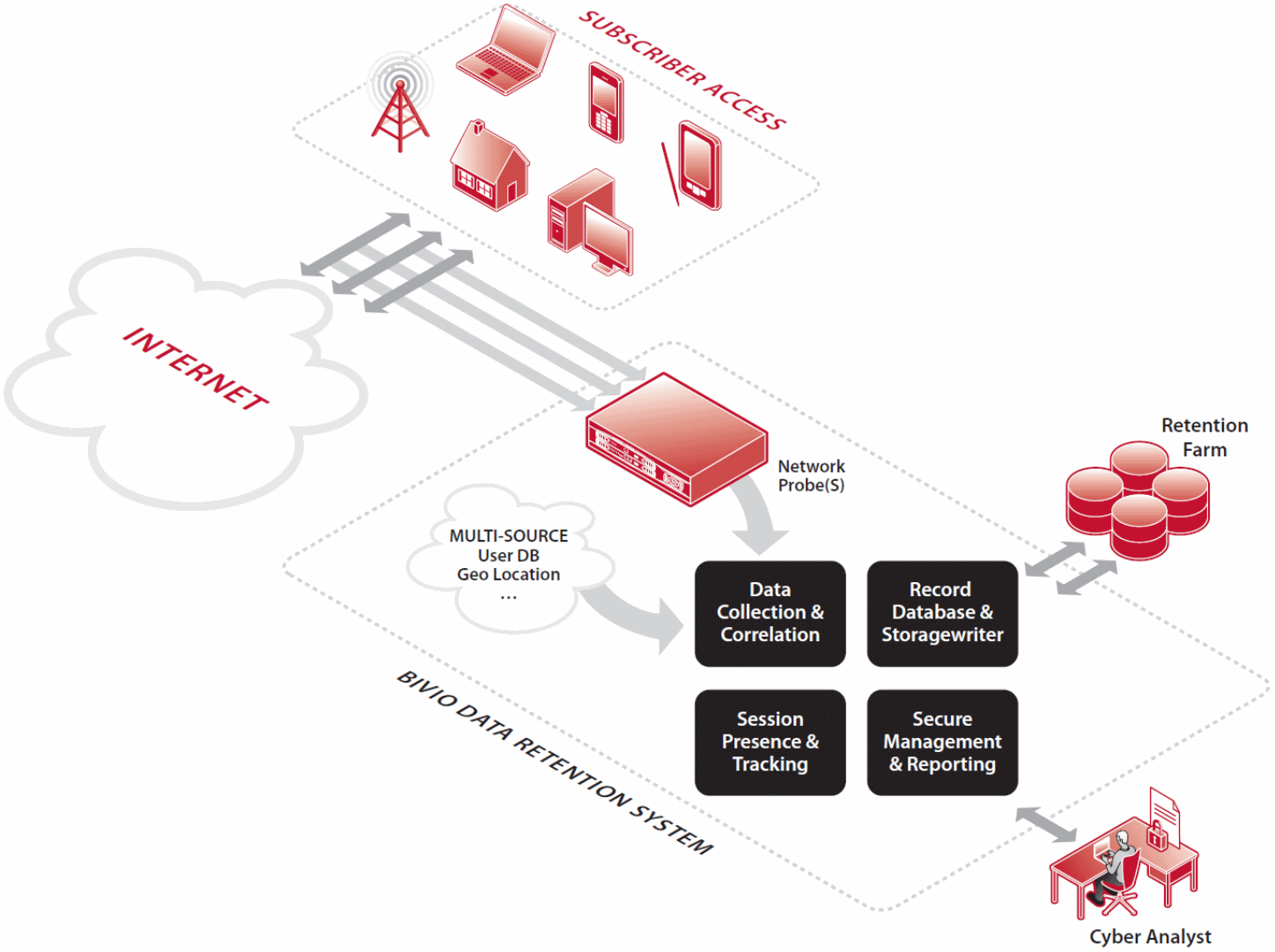
bivio networks

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

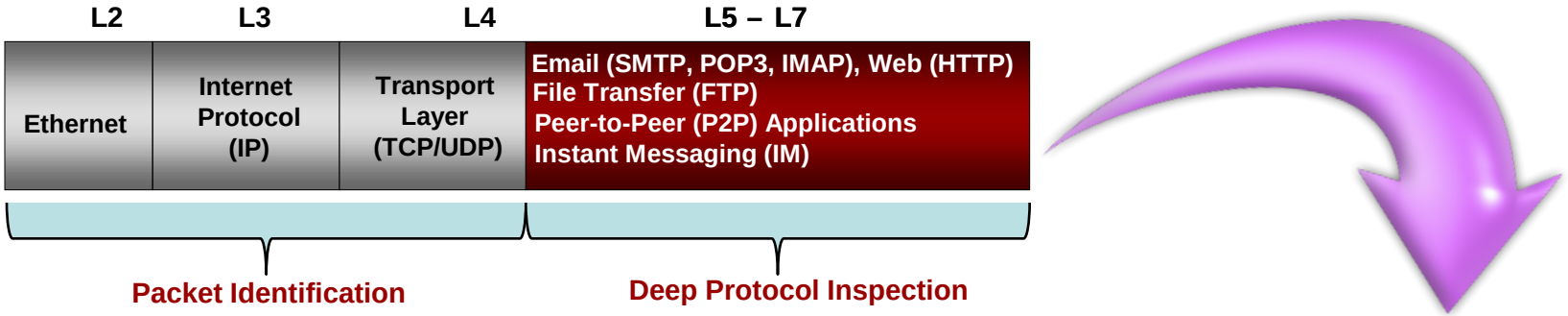
bivio networks

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

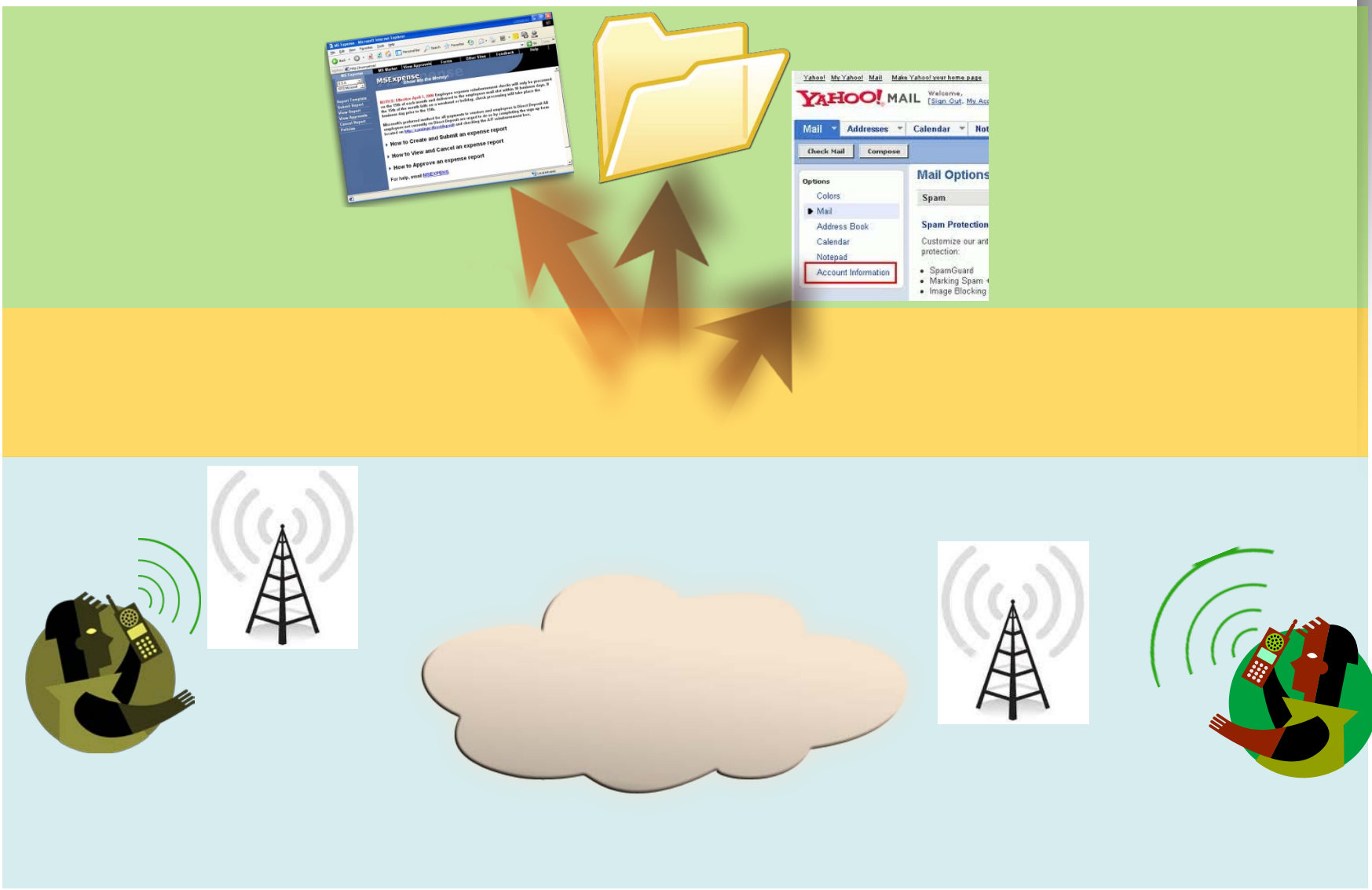


Deep Packet Inspection Probing

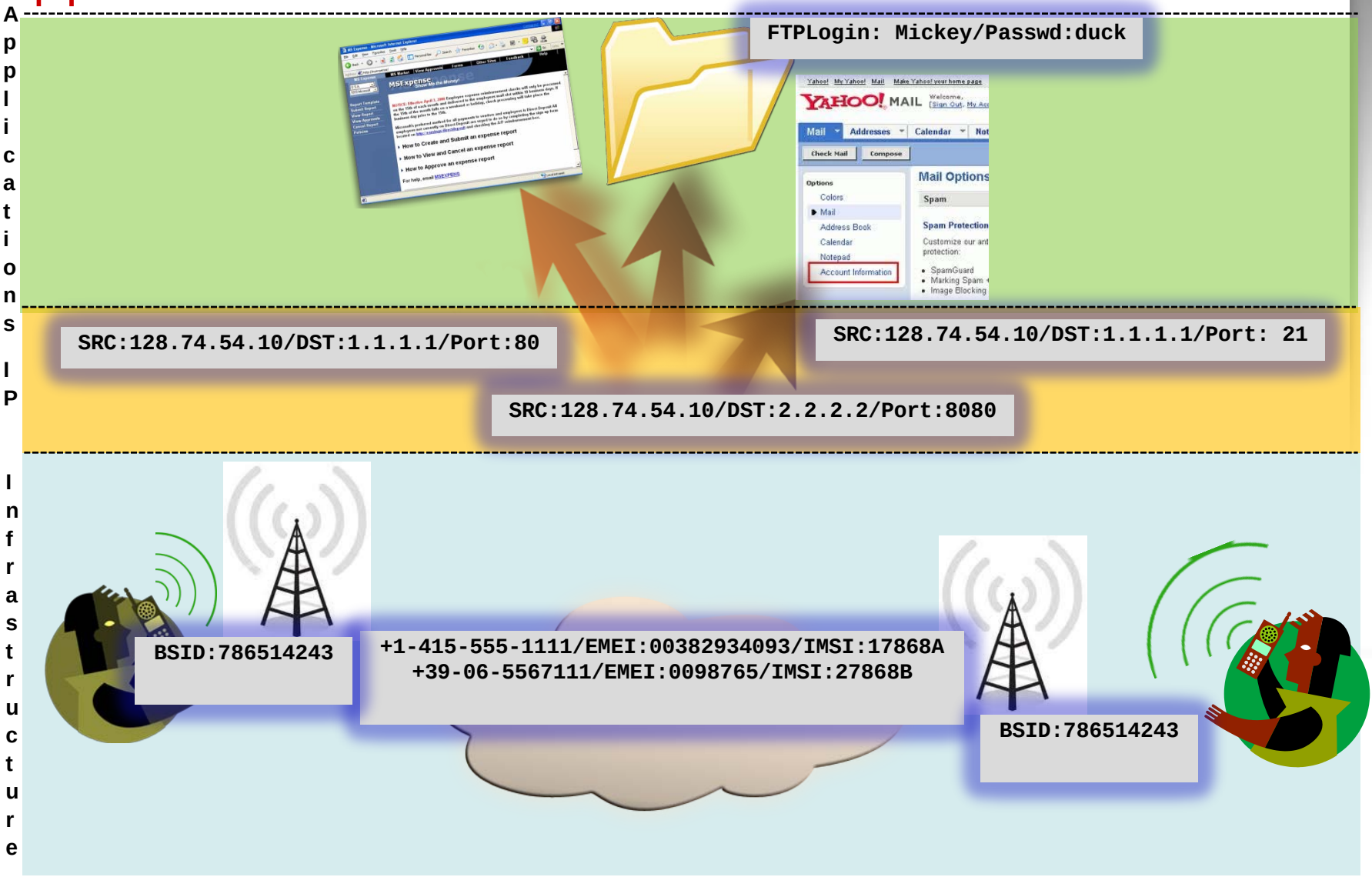
```
No.     Time        Source          Destination     Protocol Info
167207 0.756202890  10.145.19.66    10.145.19.90    GTP <HTTP> GET /img/2009/11/21/90x90-
                                                    alg_image.jpg HTTP/1.1

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 Application Inspection

Correlation Example

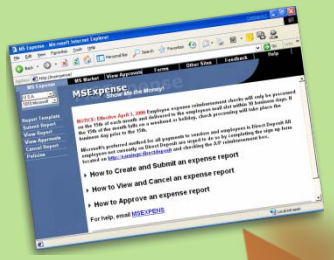


Correlation Example: Traditional DR approach



Bivio Data Retention: Correlation for Context

Application IP



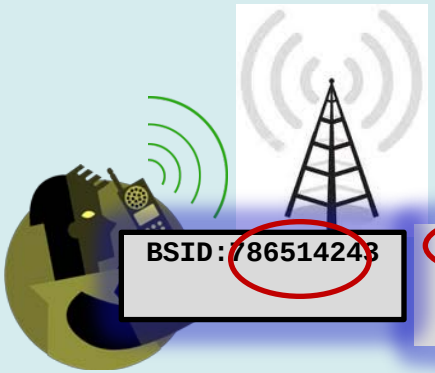
FTPLogin: Mickey/Passwd:duck: Act: put file

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

Infrastructure



BSID:78651424B

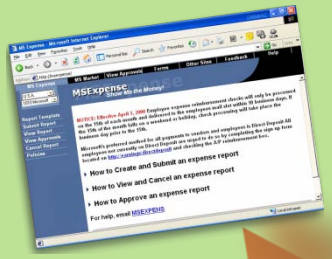
+1-415-555-1111/EMEI:00382934093/IMSI:17868A
+39-06-5567111/EMEI:0098765/IMSI:27868B

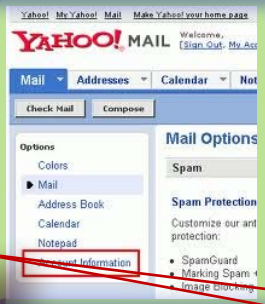
BSID:786514243

Bivio Data Retention: Correlation for Context

Application IP

Infrastructure





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/EMEI:35880801070760/IMSI:17868A
+39-06-5567111/EMEI: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 !***

bivio networks

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

bivio networks

Thank You

Joel Ebrahimi

Contact: jebrahimi@bivio.net