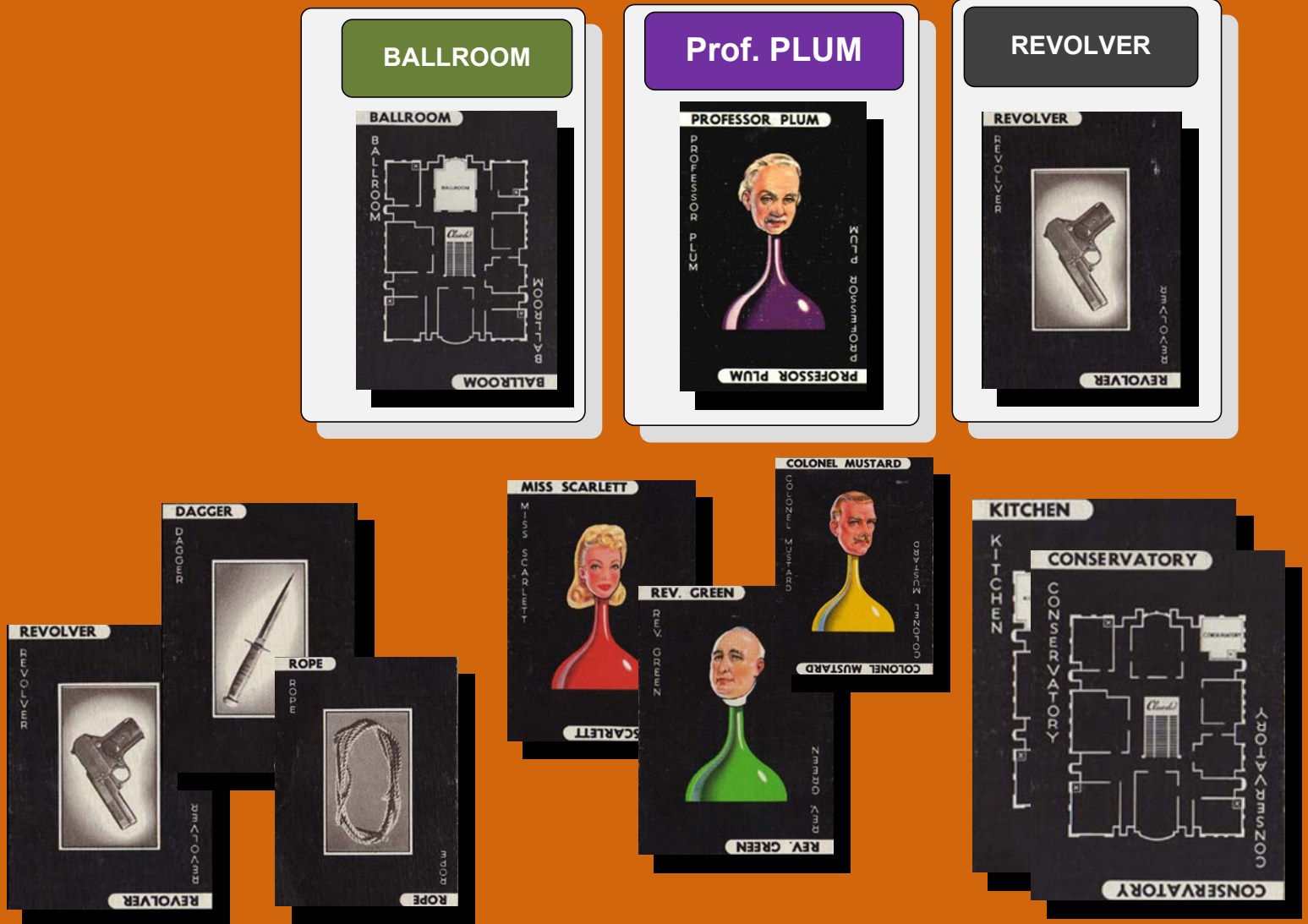
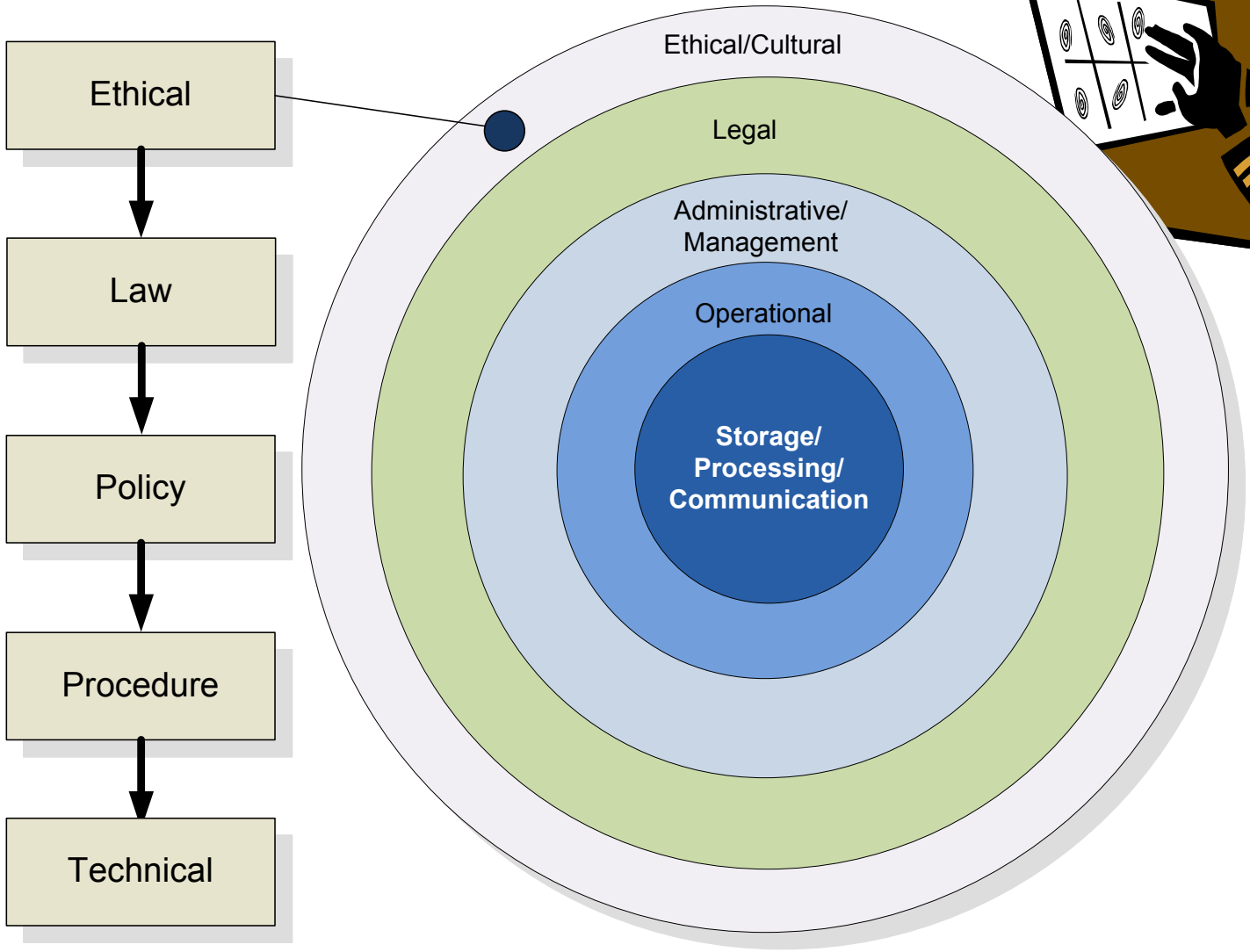
Forensic Computing



Author: Prof Bill Buchanan



Introduction

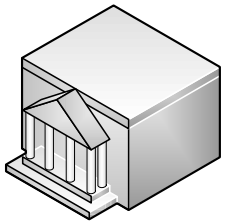
Forensic

Author: Prof Bill Buchanan

Ethical to Technical

Introduction

Forensic



Define rules, responsibilities

Report, advise

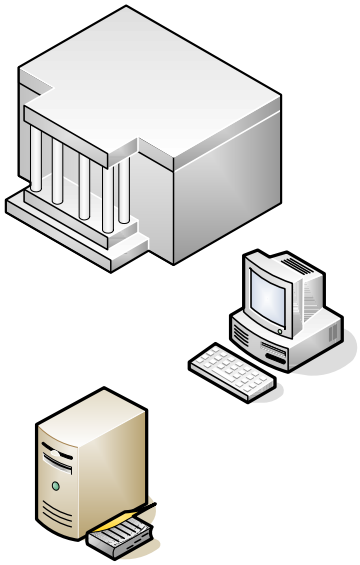
Law

Policy

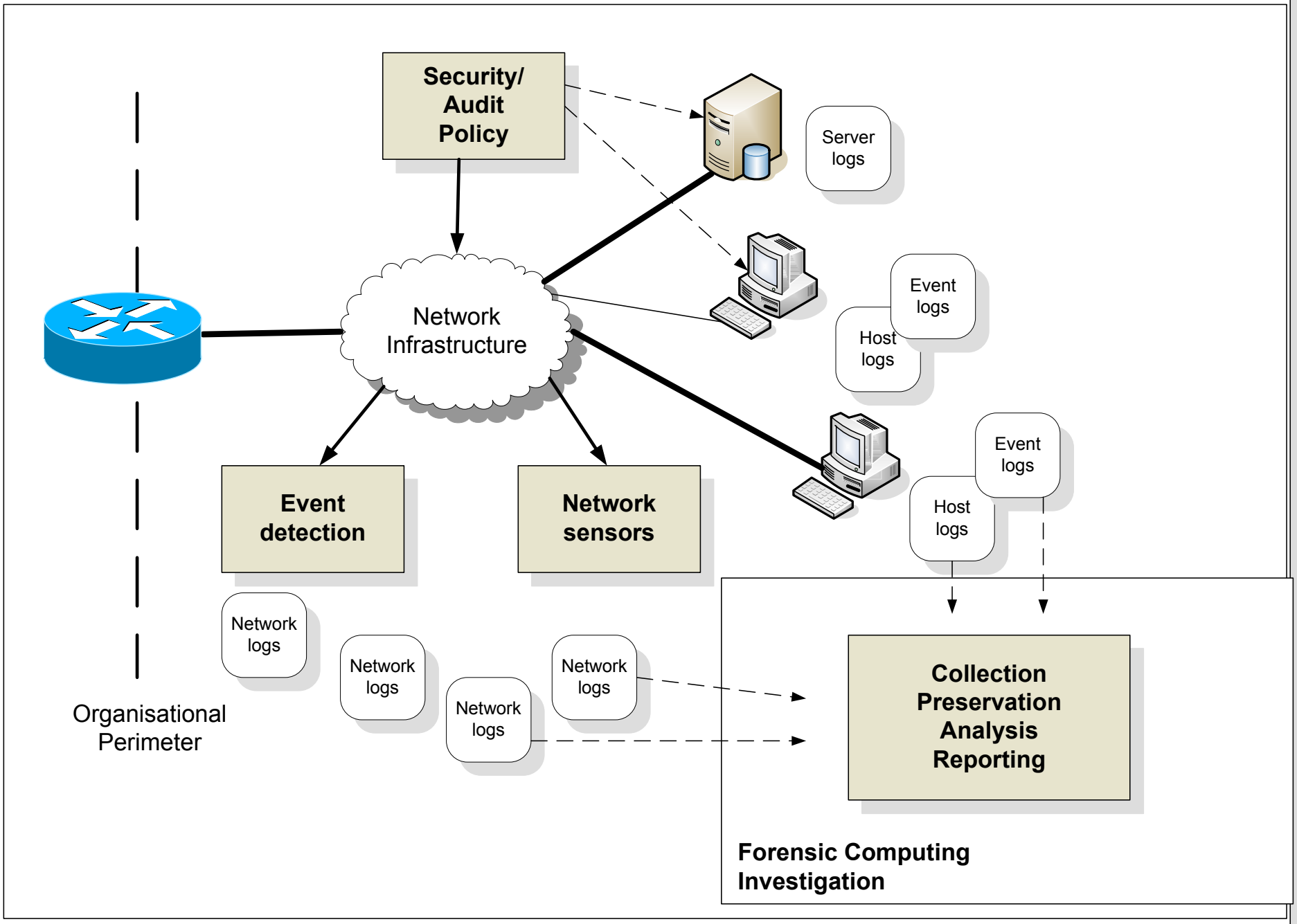
Procedure

Technical

As IT Professional, it is normally the role to translate polices into procedures. It is not normally their role to judge legal and ethical issues.



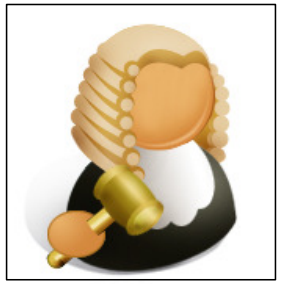
Author: Prof Bill Buchanan

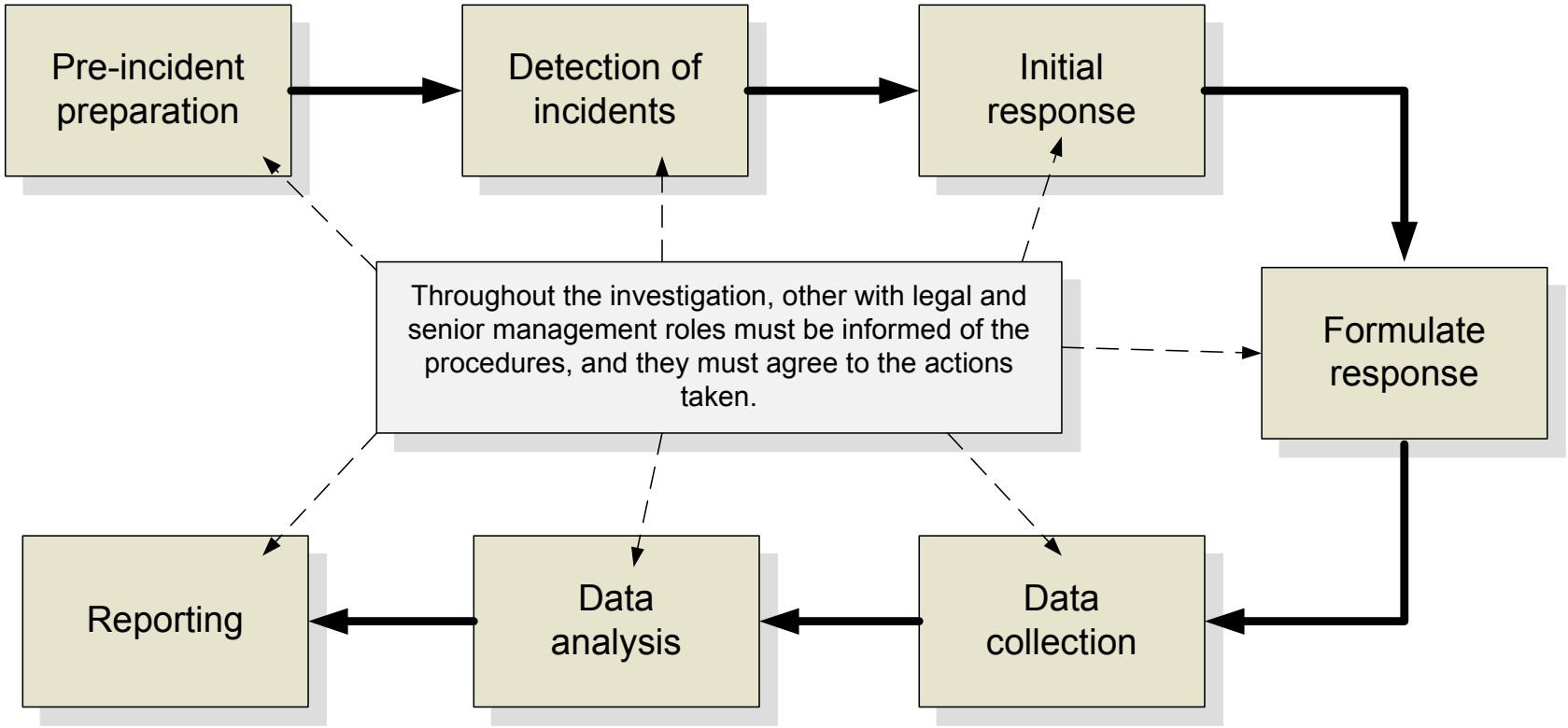


Introduction

Forensic

Author: Prof Bill Buchanan





Introduction

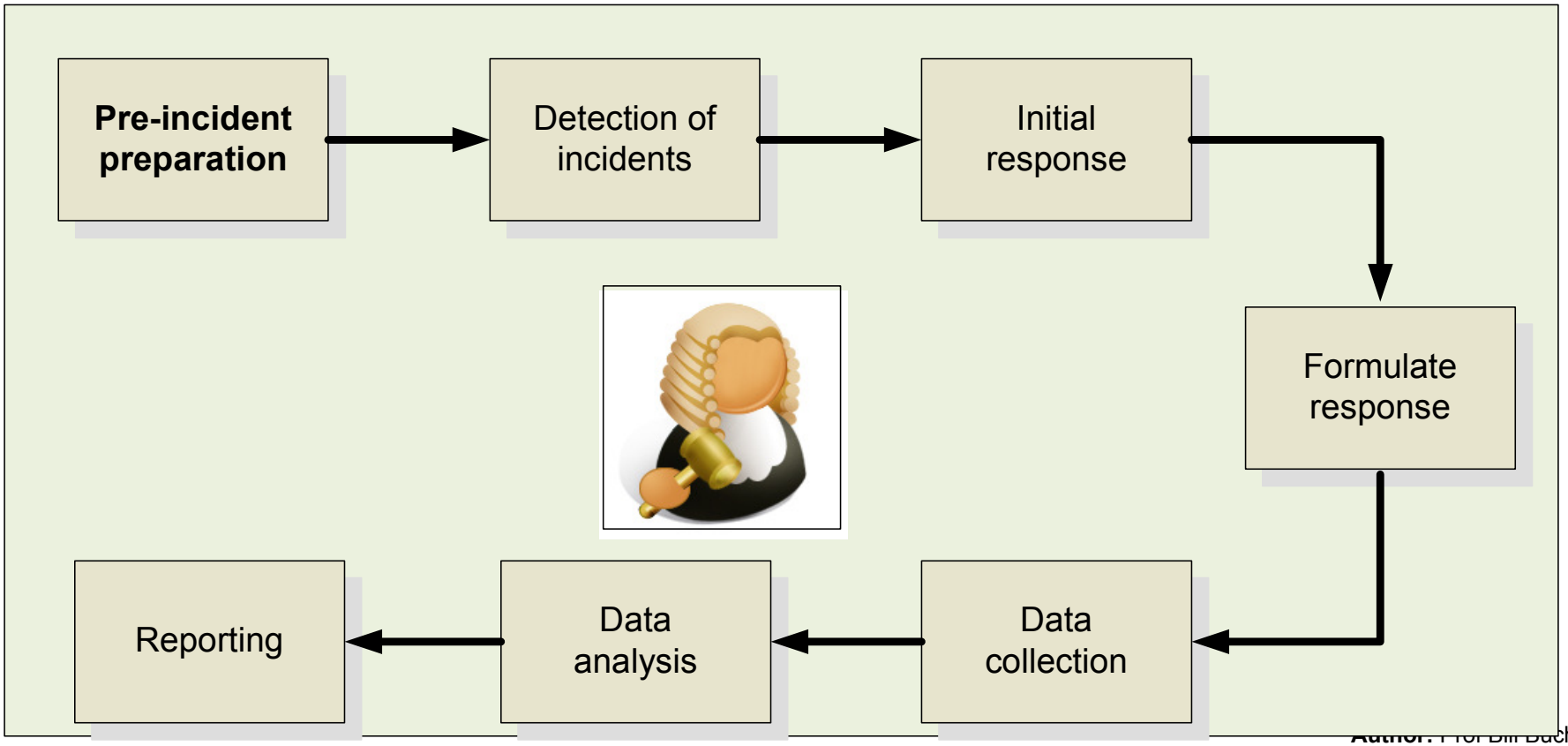
Forensic

Author: Prof Bill Buchanan

Forensic Tools

Author: Prof Bill Buchanan

- Prepare the organisation/security of potential threats.
- Define processes/responses for each threat.
- Prepare documents for audit/reporting.



Tools

Forensic

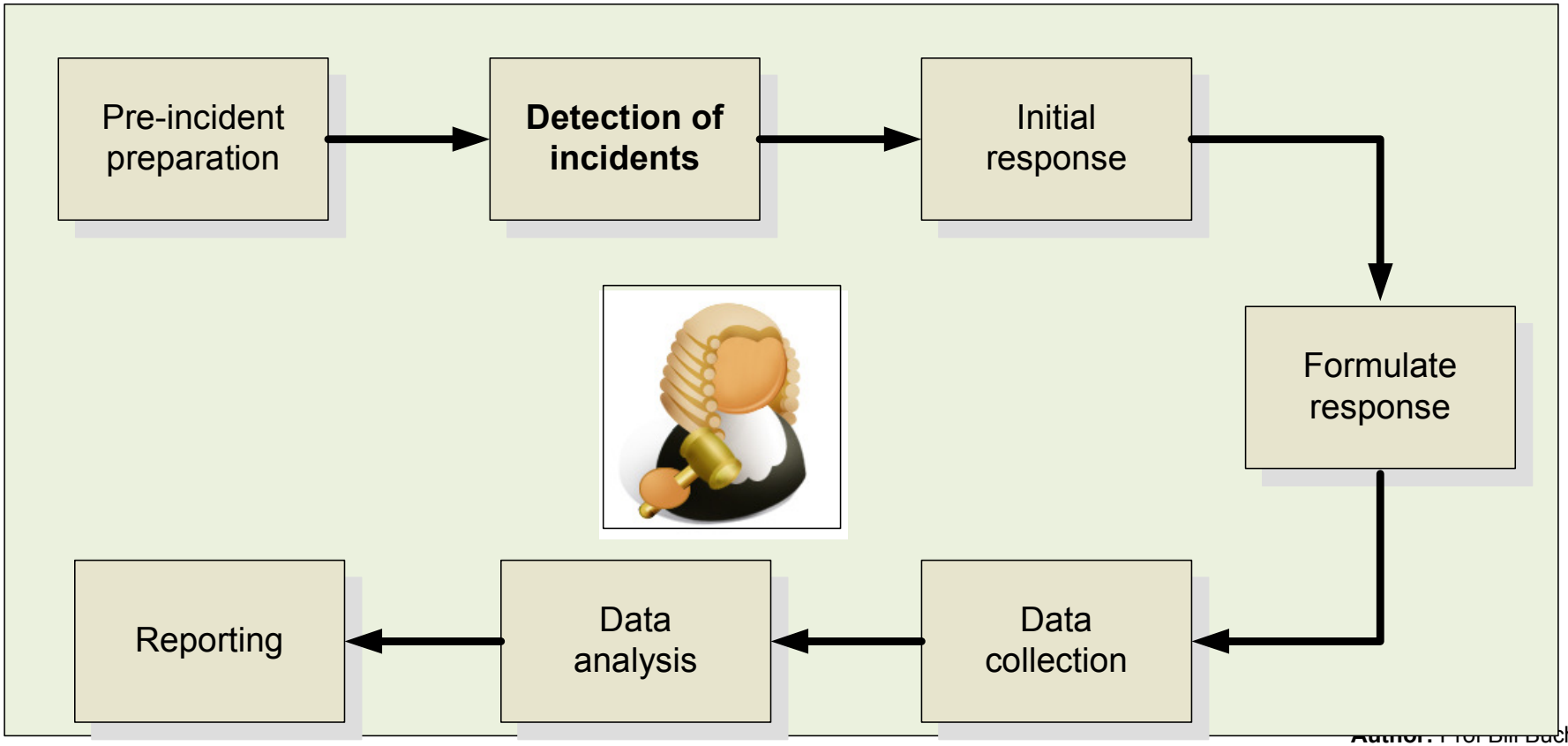
Pre-incident Preparation

Detection of incidents, such as:

- Data stealing.
- Email spam/harassment.
- Embezzlement.
- DoS Attacks/Intrusions.
- Extortion.
- Physical Damage.
- Terrorism.
- Fraud.
- Sabotage.
- Child pornography.
- Breach of contract….

Tools

Forensic



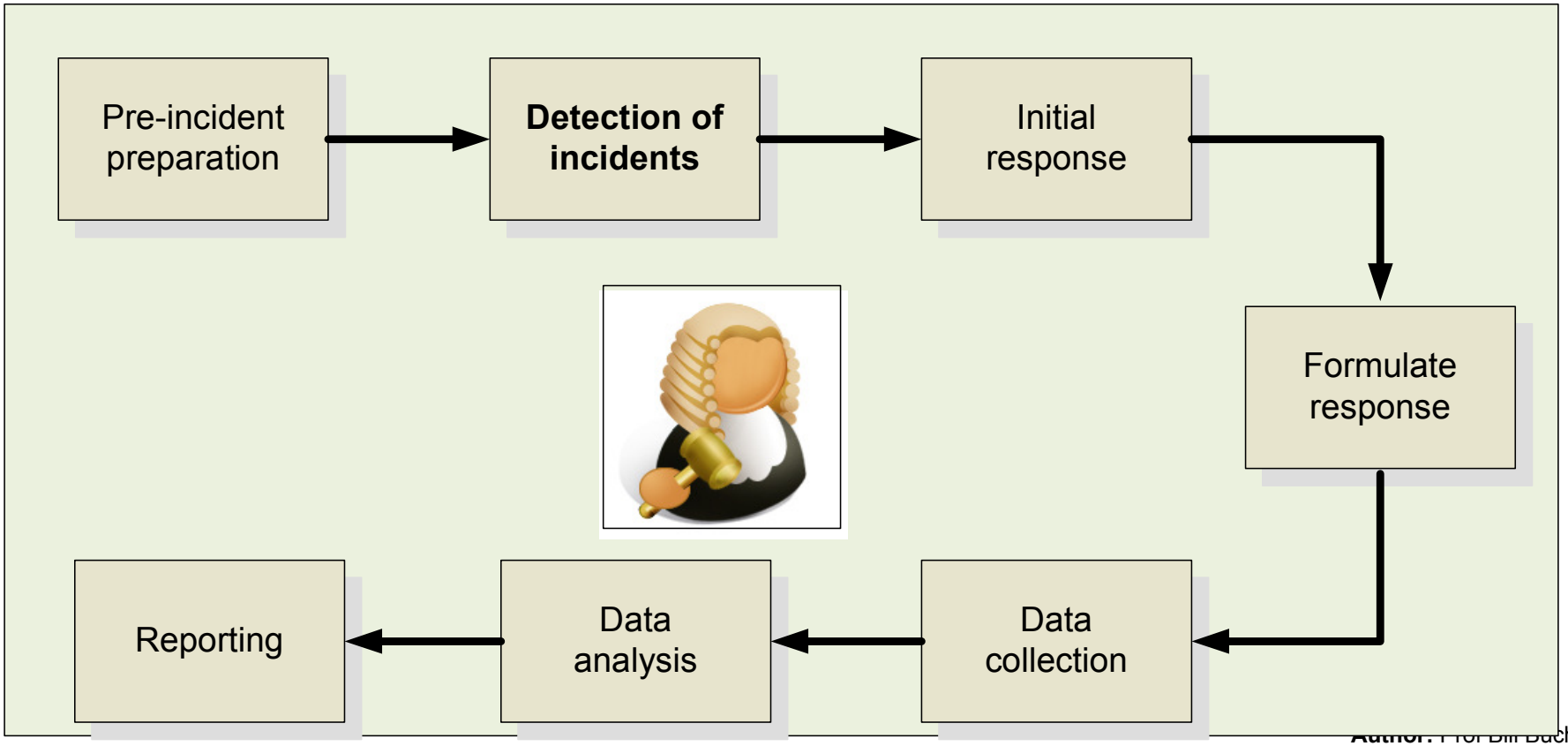
Author: Prof Bill Buchanan

Detection of Incidents

- Initial investigation, and report the incident.
  - Create a response team, and define process and activities.
  - Notify management.
  - Create an incident report.

Tools

Forensic



Author: Prof Bill Buchanan

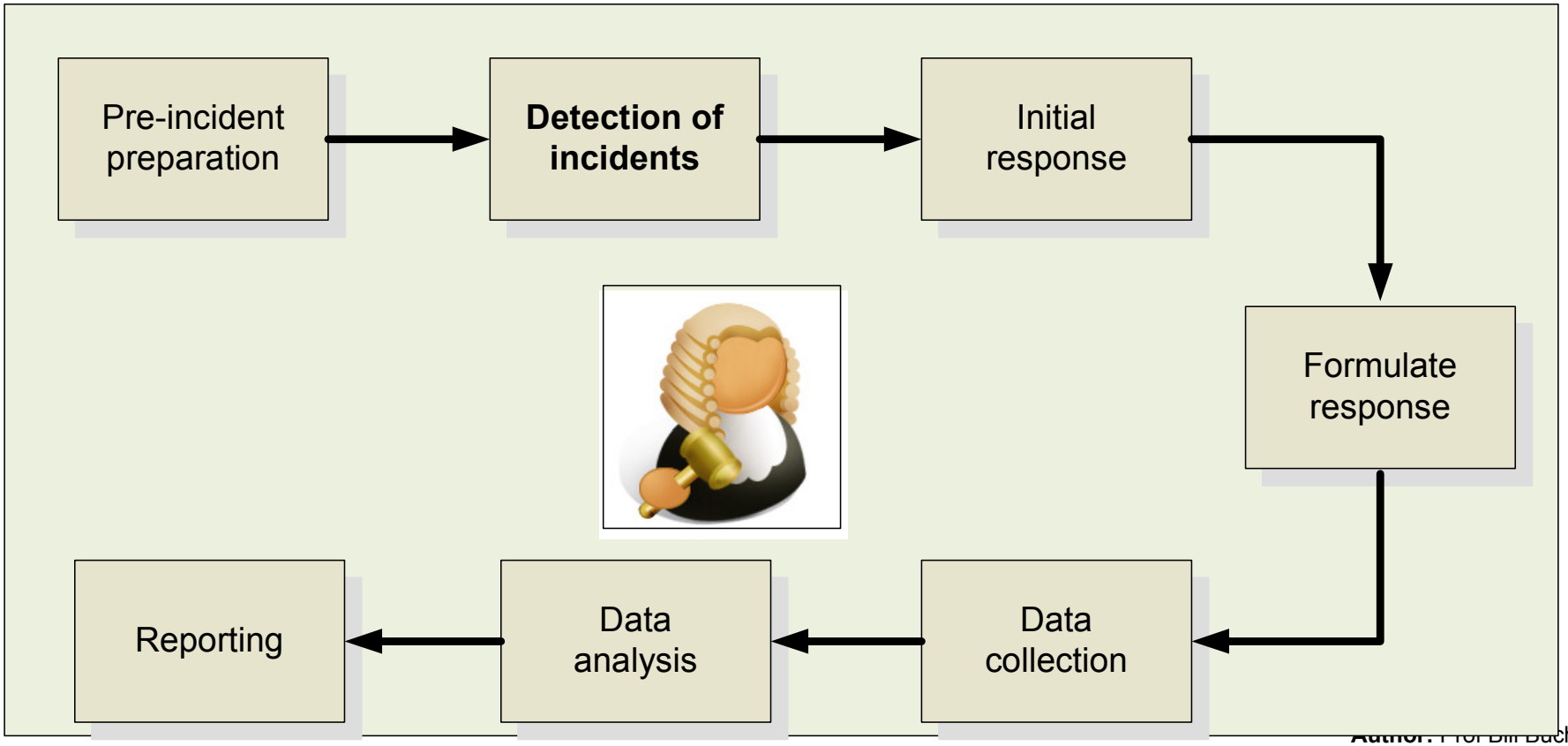
Initial Response

Define the response to the incident.

- Define civil, criminal, administrative actions.
- Obtain approval from management.

Tools

Forensic



Author: Prof Bill Buchanan

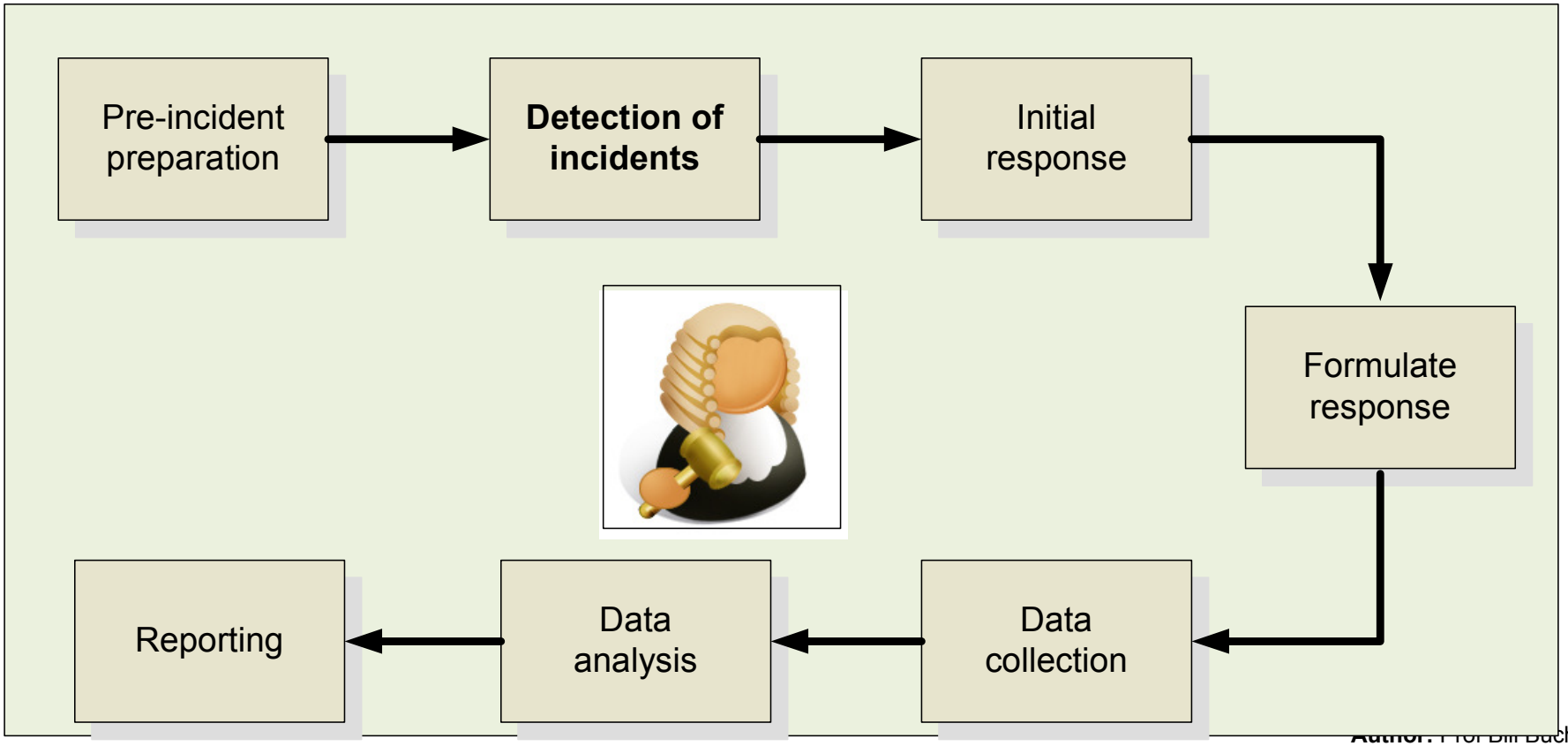
Formulate Response

Report analysis.

- Define conclusions.
- Define steps to resolve/forward incident.
- Define steps to stop incident occurring in the future.

Tools

Forensic

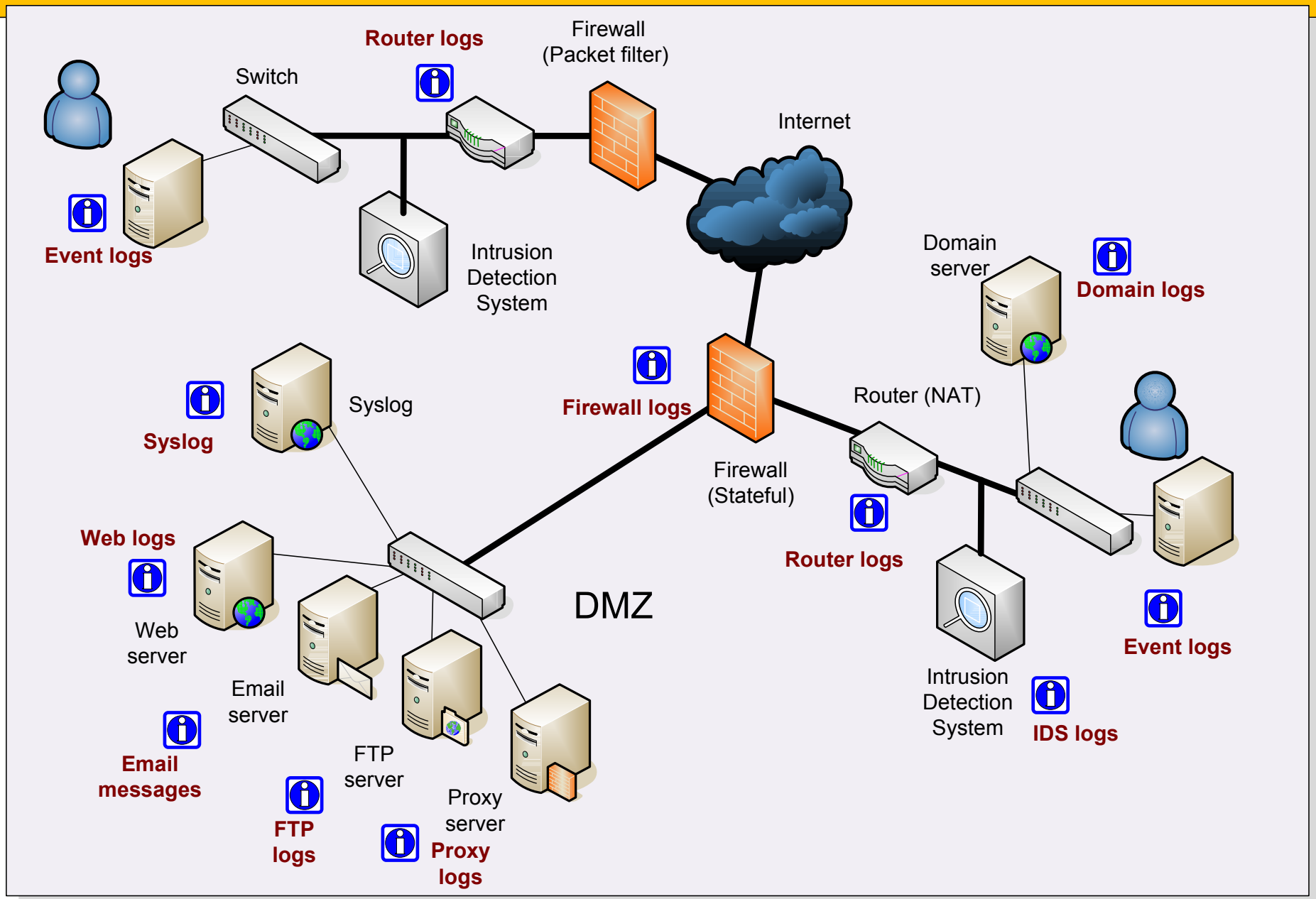


Author: Prof Bill Buchanan

Reporting

Collection

Author: Prof Bill Buchanan



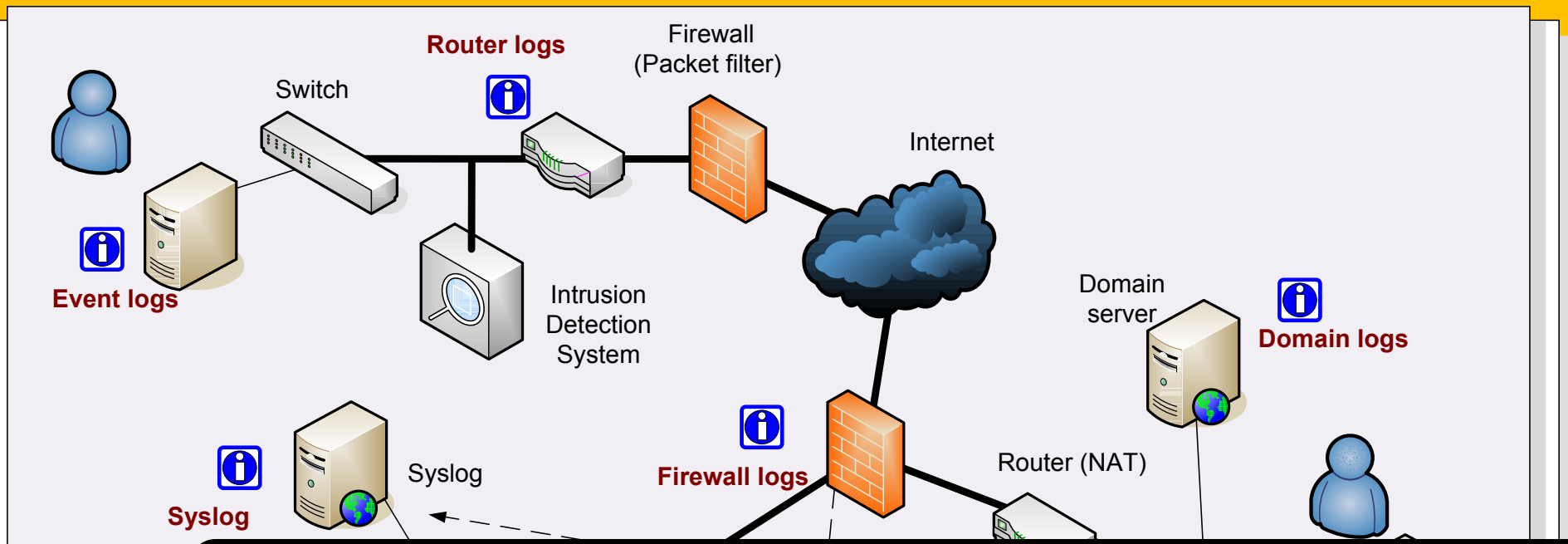
Collection

Forensic

Collection: Audit logs running on routers; Packet Monitors; Intrusion Detection Systems; Web logs; Proxy logs; Event/resource logs; and so on.

Author: Prof Bill Buchanan

Collection




```
(config)# logging on
(config)# logging 192.168.0.20
(config)# logging trap ?
  <0-7>                Logging severity level
  <4096-2147483647>    Logging buffer size
  alerts               Immediate action needed           (severity=1)
  critical             Critical conditions               (severity=2)
  debugging            Debugging messages                (severity=7)
  emergencies          System is unusable                (severity=0)
  errors               Error conditions                  (severity=3)
  informational        Informational messages            (severity=6)
  notifications        Normal but significant conditions (severity=5)
  warnings             Warning conditions                (severity=4)
  xml                  Enable logging in XML to XML logging buffer
(config)# logging trap emergency
```

Routers can be setup to sent system logging information to a remote server which supports Syslog (which is UDP port 514). The example sends to 192.168.0.20.

Author: Prof Bill Buchanan

Kiwi Syslog Service Manager (Version 7.2.35)

File Edit View Manage Help

Display 00 (Default)

Date	Time	Priority	Hostname	Message
11-26-2005	18:42:17	Local7.Notice	192.168.0.110	66: *Mar 1 04:15:31.971: %SYS-5-CONFIG_I: Configured from console by console
11-26-2005	18:42:02	Local7.Notice	192.168.0.110	65: *Mar 1 04:15:16.728: %SYS-5-CONFIG_I: Configured from console by console
11-26-2005	18:41:46	Local7.Notice	192.168.0.110	64: *Mar 1 04:15:01.365: %SYS-5-CONFIG_I: Configured from console by console

100% 3 MPH 18:42 11-26-2005

Syslog

Web log

We
serv

Ema
messa

Collection

Forensic

```
(config)# logging on
(config)# logging 192.168.0.20
(config)# logging trap ?
  <0-7>                Logging severity level
  <4096-2147483647>    Logging buffer size
  alerts               Immediate action needed           (severity=1)
  critical             Critical conditions               (severity=2)
  debugging            Debugging messages                (severity=7)
  emergencies          System is unusable                (severity=0)
  errors               Error conditions                  (severity=3)
  informational        Informational messages            (severity=6)
  notifications        Normal but significant conditions (severity=5)
  warnings             Warning conditions                (severity=4)
  xml                  Enable logging in XML to XML logging buffer
(config)# logging trap emergency
```

Routers can be setup to sent system logging information to a remote server which supports Syslog (which is UDP port 514). The example sends to 192.168.0.20.

Author: Prof Bill Buchanan

Event Viewer

File Action View Help

Event Viewer (Local)
- Custom Views
- Windows Logs
  - Application
  - Security
  - Setup
  - System
  - Forwarded Events
- Applications and Services Lo
- Subscriptions

Application 35,293 Events

Level	Date and Time	Source	Event ID	Task Cat...	User	Proces...
Information	23/11/2008 19:36:31	MSSQL...	17895	(2)	N/A	
Information	23/11/2008 19:36:31	MSSQL...	17896	(2)	N/A	
Warning	23/11/2008 19:26:18	Applic...	1	None	BILLS\bill	3844
Information	23/11/2008 19:16:31	MSSQL...	17895	(2)	N/A	
Information	23/11/2008 19:04:31	MSSQL...	17895	(2)	N/A	
Information	23/11/2008 18:56:31	MSSQL...	17895	(2)	N/A	
Information	23/11/2008 18:44:31	MSSQL...	17895	(2)	N/A	
Information	23/11/2008 18:32:31	MSSQL...	17895	(2)	N/A	
Information	23/11/2008 18:32:31	MSSQL...	17896	(2)	N/A	
Information	23/11/2008 17:47:41	MSSQL...	17895	(2)	N/A	
Information	23/11/2008 17:35:41	MSSQL...	17895	(2)	N/A	
Information	23/11/2008 17:31:41	MSSQL...	17895	(2)	N/A	

Event 17895, MSSQL$SQLEXPRESS

General Details

CPU time stamp frequency has changed from 688788 to 809822 ticks per millisecond. The new frequency will be used.

Log Name: Application

Actions

Application
- Open Saved Log...
- Create Custom View...
- Import Custom Vie...
- Clear Log...
- Filter Current Log...
- Properties
- Find...
- Save Events As...
- Attach a Task To thi...
- View
- Refresh
- Help

Event 17895, MSSQL$SQL...
- Event Properties
- Attach Task To This ...
- Copy
- Save Selected Event...
- Refresh

Collection

Forensic

Author: Prof Bill Buchanan

Windows Event Log (Application)

Event Viewer

File Action View Help

Event Viewer (Local)
- Custom Views
- Windows Logs
  - Application
  - Security
  - Setup
  - System
  - Forwarded Events
- Applications and Services Lo
- Subscriptions

Security 1,505 Events

Keywor...	Level	Date and Time	Source	Event ID	Task Categ...	User
Audi...	Information	23/11/2008 18:24:07	Micros...	4776	Credential ...	N/A
Audi...	Information	23/11/2008 13:43:42	Micros...	4776	Credential ...	N/A
Audi...	Information	22/11/2008 19:19:56	Micros...	4776	Credential ...	N/A
Audi...	Information	22/11/2008 14:59:50	Micros...	4776	Credential ...	N/A
Audi...	Information	21/11/2008 21:20:38	Micros...	4776	Credential ...	N/A
Audi...	Information	21/11/2008 21:19:16	Micros...	4616	Security St...	N/A
Audi...	Information	21/11/2008 21:19:16	Eventlog	1100	Service shu...	N/A
Audi...	Information	21/11/2008 21:17:25	Micros...	4776	Credential ...	N/A
Audi...	Information	21/11/2008 11:41:50	Micros...	4776	Credential ...	N/A
Audi...	Information	21/11/2008 10:04:08	Micros...	4776	Credential ...	N/A
Audi...	Information	21/11/2008 09:42:10	Micros...	4776	Credential ...	N/A
Audi...	Information	21/11/2008 08:48:48	Micros...	4776	Credential ...	N/A

Event 4776, Microsoft Windows security auditing.

General Details

The domain controller attempted to validate the credentials for an account.

Authentication Package: MICROSOFT_AUTHENTICATION_PACKAGE_V1_0

Log Name: Security

Actions

Security
- Open Saved Log...
- Create Custom View...
- Import Custom Vie...
- Clear Log...
- Filter Current Log...
- Properties
- Find...
- Save Events As...
- Attach a Task To thi...
- View
- Refresh
- Help

Event 4776, Microsoft Wi...
- Event Properties
- Attach Task To This ...
- Copy
- Save Selected Event...
- Refresh

Saves the log under a different name.

Collection

Forensic

Author: Prof Bill Buchanan

Windows Event Log (Security)

```
C:\Windows\System32\config>dir *.evt

04/07/2008  22:32          524,288 AppEvent.Evt
11/05/2008  08:18           65,536 Internet.evt
11/05/2008  11:18           65,536 ODiag.evt
26/06/2008  19:30           65,536 OSession.evt
04/07/2008  22:32          327,680 SecEvent.Evt
04/07/2008  15:55          524,288 SysEvent.Evt
```

Event Viewer

File Action View Help

Event Viewer (Local)
- Custom Views
- Windows Logs
  - Application
  - Security
  - Setup
  - System
  - Forwarded Events
- Applications and Services Lo
- Subscriptions

System 41,802 Events

Level	Date and Time	Source	Event ID	Task C...	User
Information	12/11/2008 10:39:11	EventL...	6013	None	N/A
Information	12/11/2008 10:39:11	EventL...	6005	None	N/A
Information	12/11/2008 10:39:11	EventL...	6009	None	N/A
Information	12/11/2008 10:38:00	EventL...	6006	None	N/A
Information	12/11/2008 08:19:41	EventL...	6013	None	N/A
Information	12/11/2008 08:19:41	EventL...	6005	None	N/A
Information	12/11/2008 08:19:41	EventL...	6009	None	N/A
Error	12/11/2008 08:19:41	EventL...	6008	None	N/A
Warning	12/11/2008 08:19:27	b57nd6...	4	None	N/A
Information	12/11/2008 08:19:23	b57nd6...	15	None	N/A
Information	12/11/2008 08:19:23	NETw4...	7036	None	N/A
Information	12/11/2008 08:19:22	Kernel-...	4	None	SYSTEM
Information	12/11/2008 08:19:22	Kernel-...	4	None	SYSTEM

Event 6013, EventLog

General Details

The system uptime is 24 seconds.

Log Name: System

Actions

System
- Open Saved Log...
- Create Custom View...
- Import Custom Vie...
- Clear Log...
- Filter Current Log...
- Properties
- Find...
- Save Events As...
- Attach a Task To thi...
- View
- Refresh
- Help

Event 6013, EventLog
- Event Properties
- Attach Task To This ...
- Copy
- Save Selected Event...
- Refresh

Collection

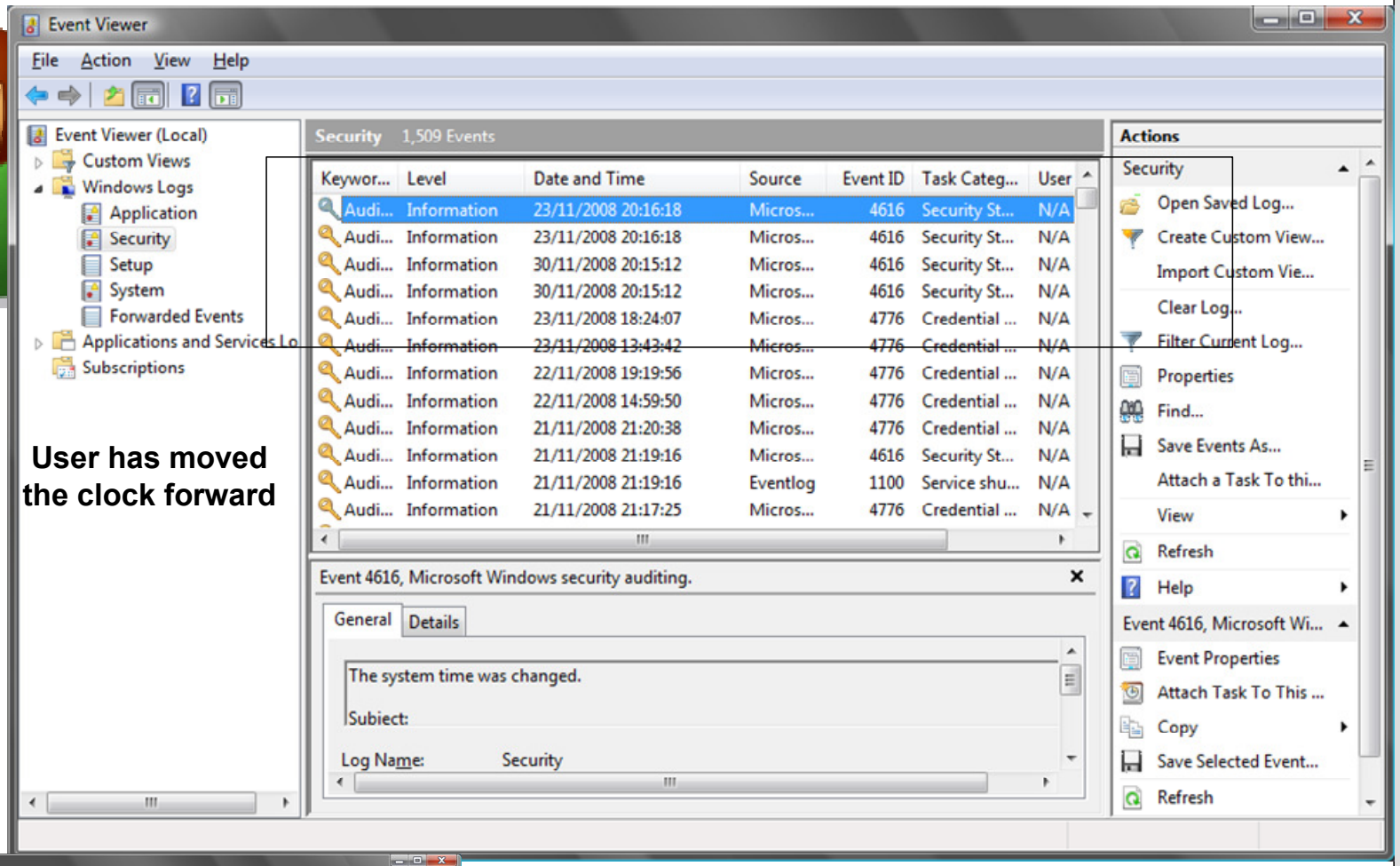
Forensic

Author: Prof Bill Buchanan

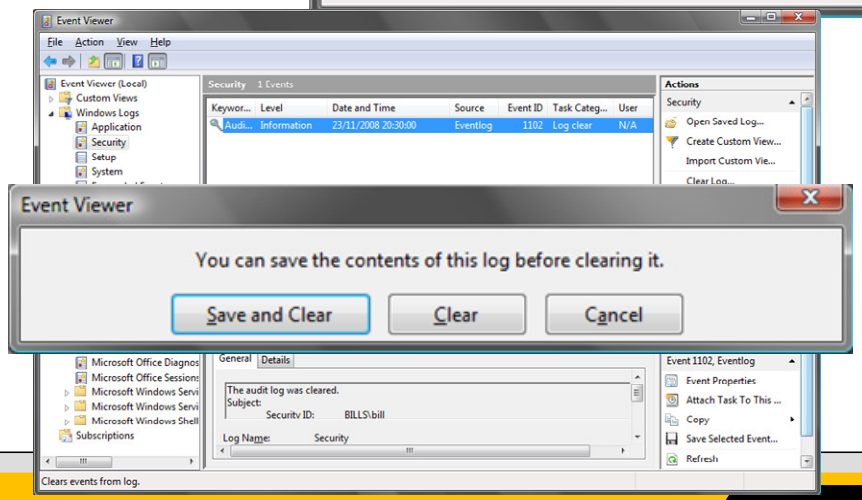
Windows Event Log (System)

Collection

Forensic



User has moved the clock forward

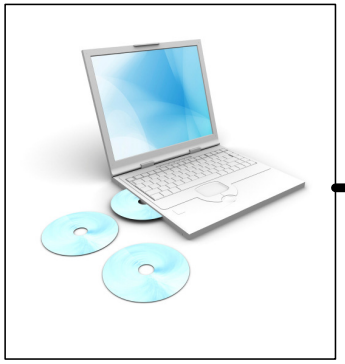


Author: Prof Bill Buchanan

Problems

Preservation

Author: Prof Bill Buchanan



Time stamp files → Hash signature → Mirror data → Store data

A key element is the preservation and validation of data. Thus data must be time stamped and validated.

```
C:\www>md5 *.html
7D0F73144AEDAF037147258C563A7959  404.html
5B61DD53B7A206496A7074225AAE257F  active_directories.html
CEDE68C1D8A5119889BE28F69F60EAC0  ad_arc.html
AD81F20B8AE407BE959997F129056E3B  ad_form.html
7EC1053391DD226834D98B6C151EA257  adcbook.html
7C1DCB92E205D1398AD63D4911403898  adcbook1.html
D2E6EBD20AAAADE01DC79480F2C8F498  adpcbook.html
C12BDD1533DDB1529E299C838E7A056D  apcbook.html
0A1091032BE1B7A07ABD5BCEC6904DC1  apcbook1.html
FEB0C01B366ECD6D81FD0F908466F6B6  asmn.html
583C036086049E1DD5A9319578F99765  asmn_activities_week.html
23A8E4119BC3F8BCC5BA6C7A9492FF5D  asmn_mo.html
8ABCFB4143EC7D93FE43B219578EF809  asmn_notes.html
```

128-bit fingerprint of files (3.40×10^{34})

Preservation

Forensic

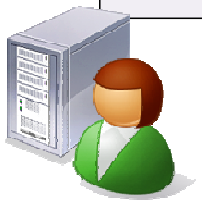
Author: Prof Bill Buchanan

Preservation

Automated script written, which does the following:

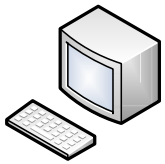
1. Details of incident taken (IP address, MAC address, and so on).
2. Directory listing taken.
3. MD5 fingerprint taken for each file.
4. Files ZIP'ed into a single folder, with full path names.

and so on.



Report_host_date_time.txt

Files_host_date_time.txt



Host-under-investigation

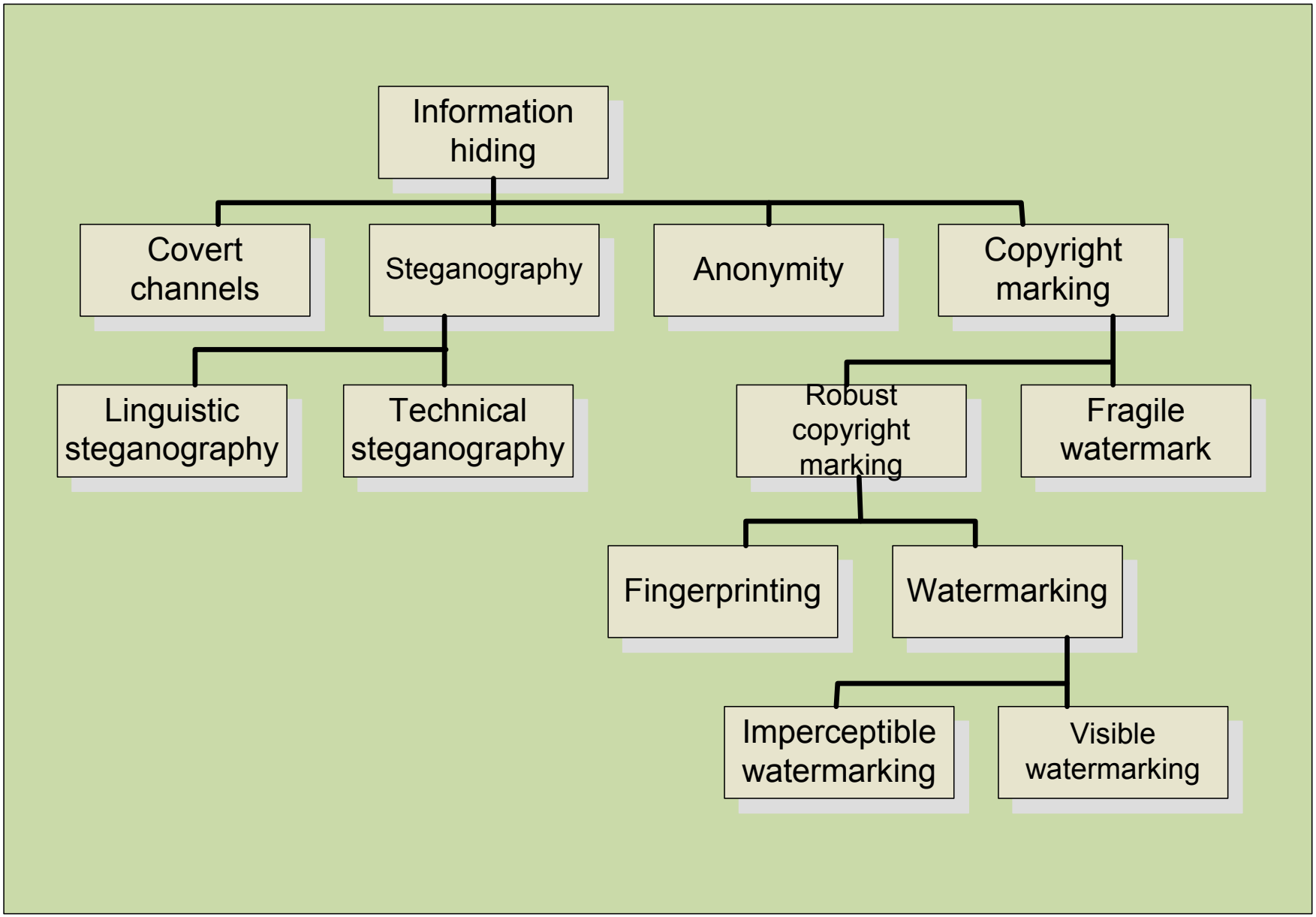
Backup storage

```
echo Date > report_host_date_time.txt
date >> report_host_date_time.txt
echo Time >> report_host_date_time.txt
time >> report_host_date_time.txt
echo IPCONFIG details >> report_host_date_time.txt
ipconfig /all >> report_host_date_time.txt
echo Directory Listing >> report_host_date_time.txt
dir /s >> report_host_date_time.txt
md5 *.* /s >> report_host_date_time.txt
zip *.* /s >> files_host_date_time.txt
md5 files_host_date_time.zip >> report_host_date_time.txt
… etc
```

Author: Prof Bill Buchanan

Data Hiding

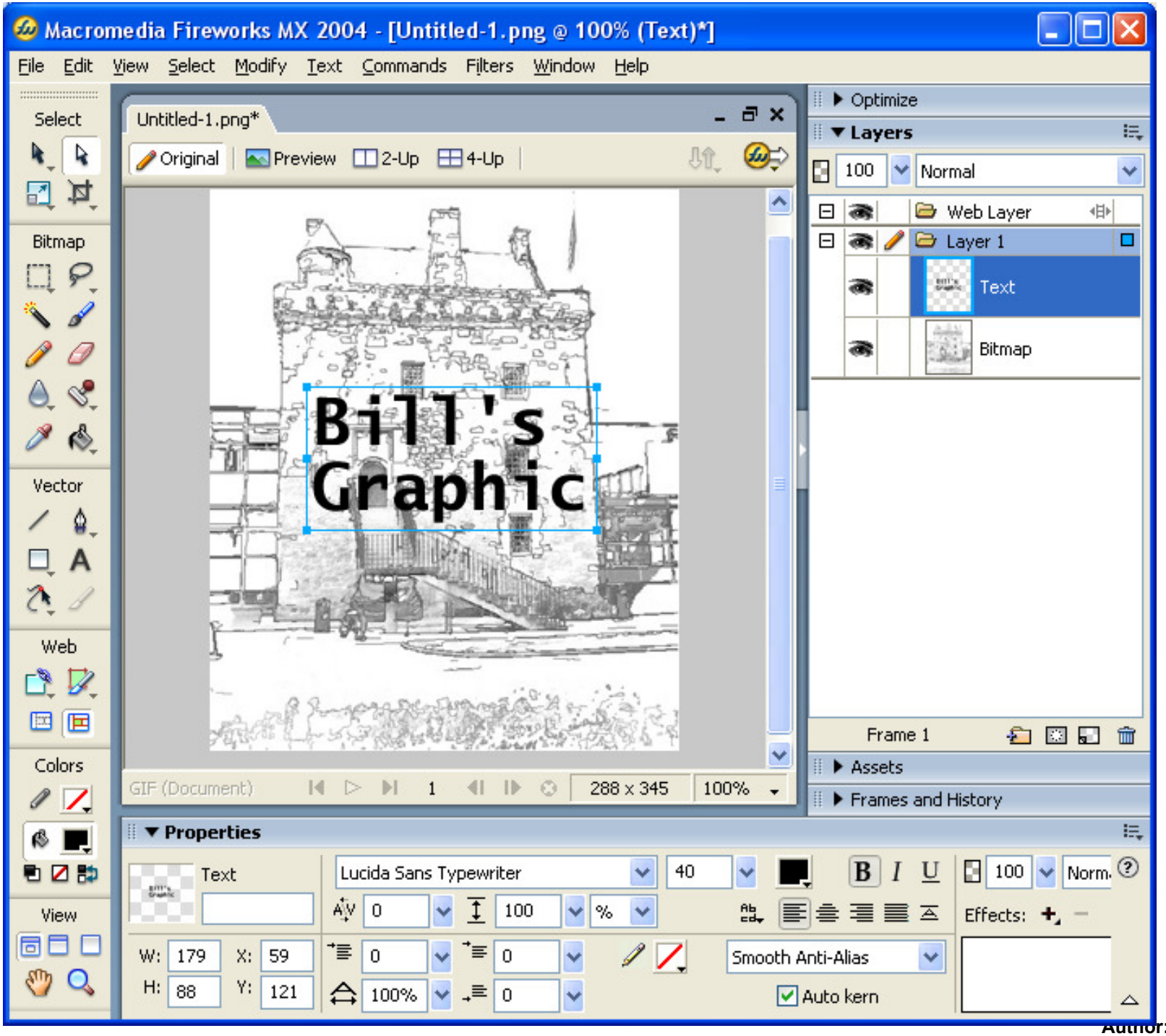
Author: Prof Bill Buchanan



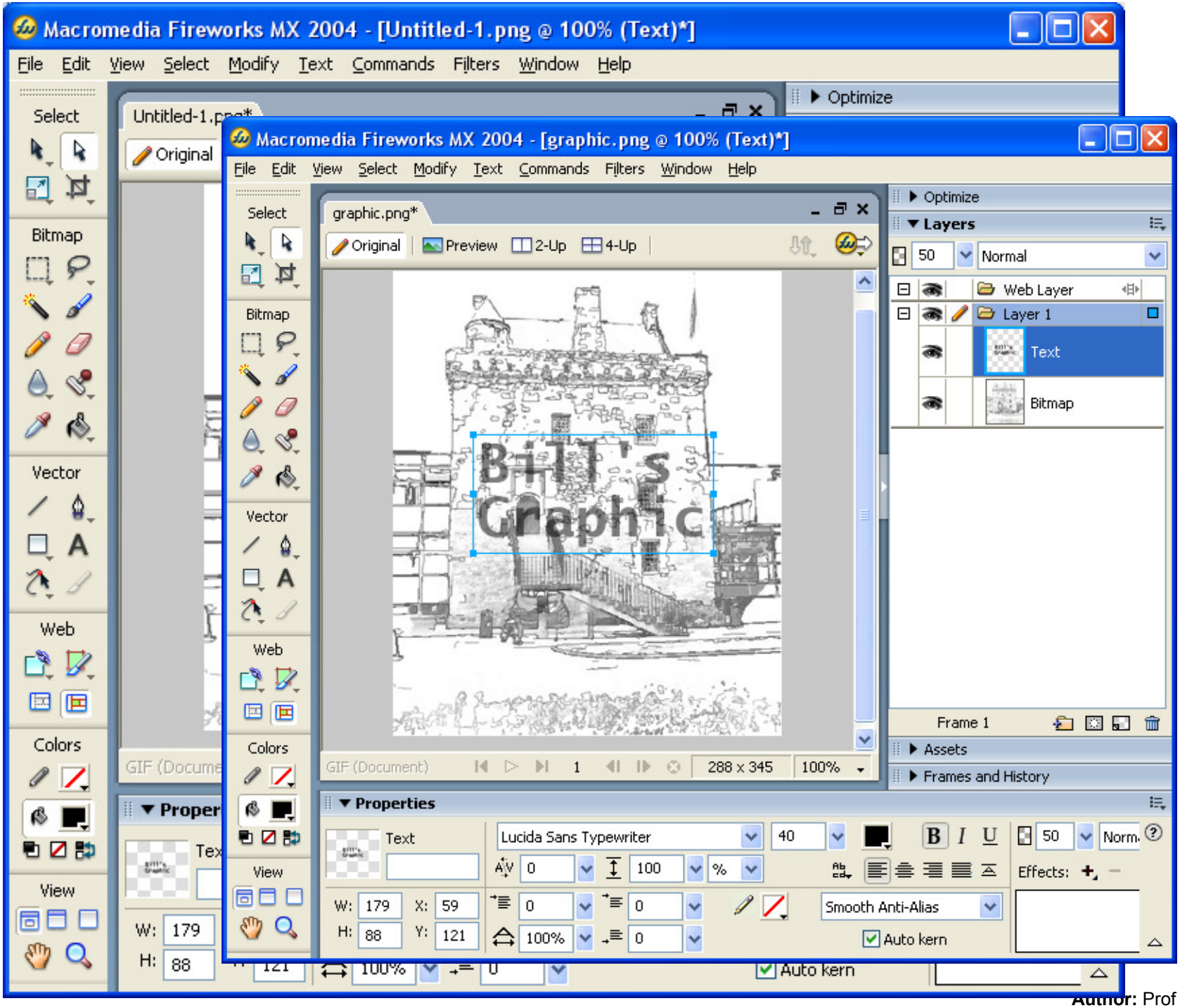
Data hiding

Forensic

Author: Prof Bill Buchanan

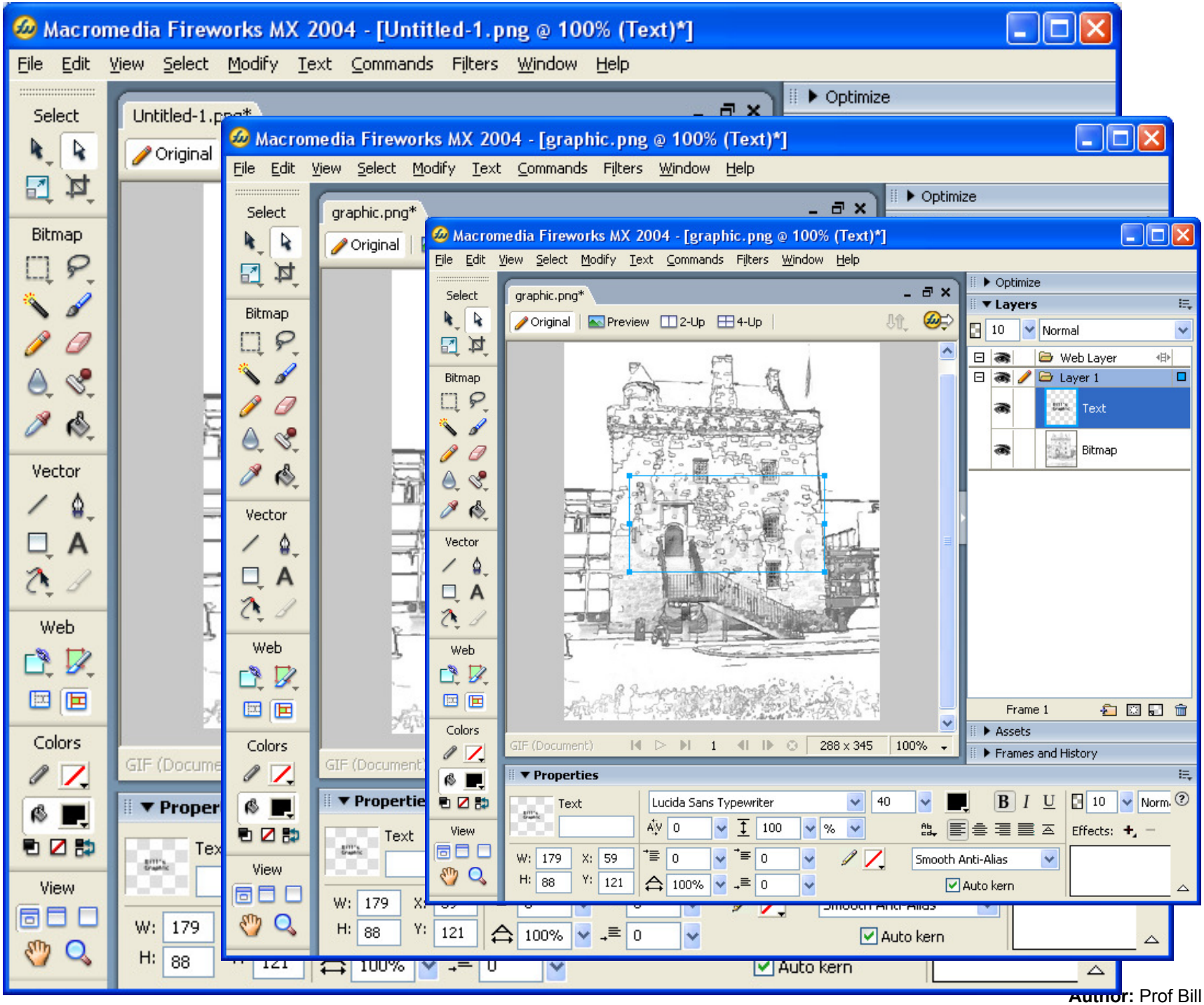


Author: Prof Bill Buchanan



Author: Prof Bill Buchanan

Data Hiding

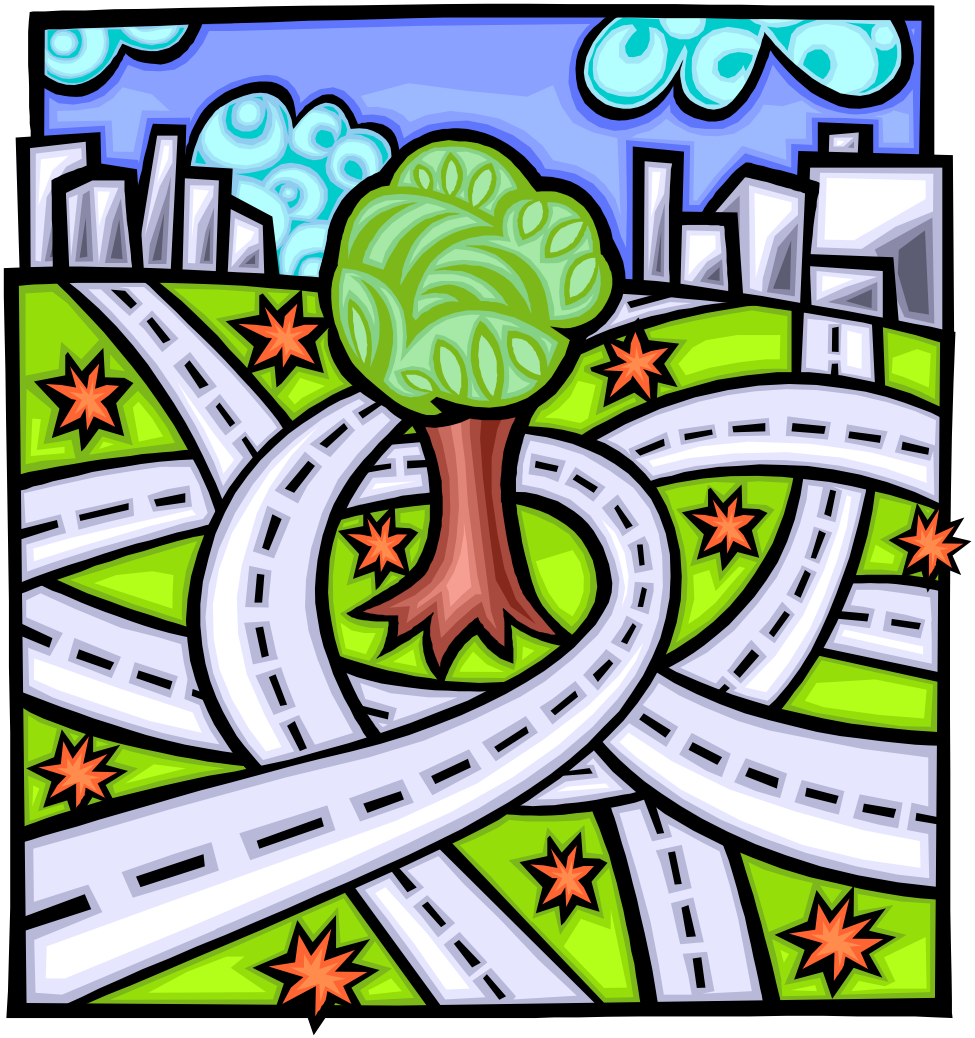


Author: Prof Bill Buchanan

Data Hiding

Obfuscation

Author: Prof Bill Buchanan

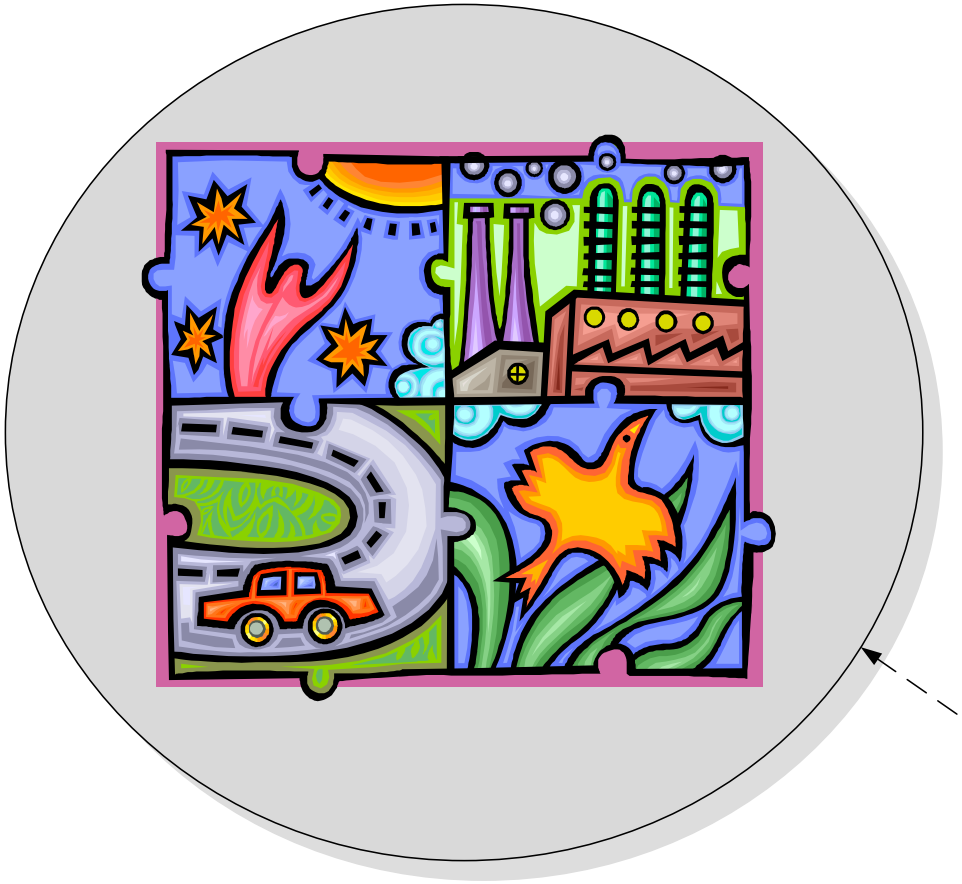


Author: Prof Bill Buchanan

Obfuscation

Forensic

Author: Prof Bill Buchanan



Author: Prof Bill Buchanan

Obfuscation

Forensic

Mypic.gif

↓

Mypic.dll

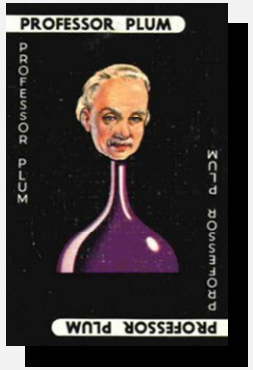
Change name from:

Mypic.gif

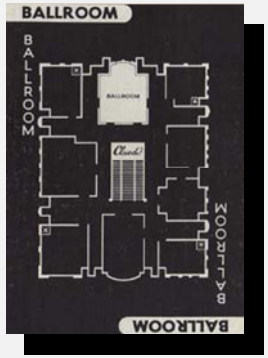
To

Mypic.dll

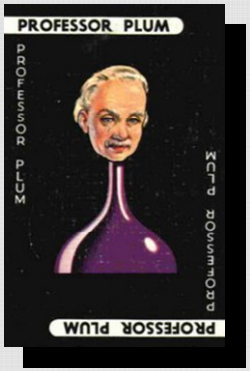
Prof. PLUM



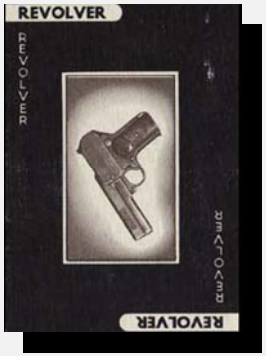
BALLROOM



Prof. PLUM



REVOLVER



File name changing

Obfuscation

Forensic

Mypic.gif

Mypic.dll

GIF89a….

Free Hex Editor Neo

File Edit View Select Operations Bookmarks NTFS Streams Tools History Window Help

cat01_old.gif

	00 01 02 03	04 05 06 07	08 09 0a 0b	0c 0d 0e 0f	
00000004	47 49 46 38	39 61 64 00	55 00 e6 00	00 ff ff ff	GIF89ad.U.æ..ÿÿÿ
00000010	f7 f7 f6 f1	f4 f2 ee ee	ef e7 e7 e7	e1 e4 e6 df	÷÷öñôòîîïçççáäæß
00000020	de df d7 da	dd ef ce ce	d5 d5 d5 d5	d3 d0 d9 d1	Þß×ÚÝïÎÎÕÕÕÕÓÐÙÑ
00000030	a1 cc cc cc	c4 c8 cc 68	65 6c 6c 6f	c0 d1 c6 84	¡ÌÌÌÄÈÌhelloÀÑÆ„
00000040	c0 bf bd bd	bb b8 b8 b6	b5 b5 b3 ae	aa b1 b6 ab	À¿½½»¸¸¶µµ³®ª±¶«
00000050	ac ad ab a9	a5 a6 a6 a6	a7 a5 9e ab	a8 70 ac 9c	¬-«©¥¦¦¦§¥ž«¨p¬œ
00000060	9f 99 99 99	94 9a a0 8b	95 9c 93 92	8e 8c 8d 8a	Ÿ™™™”š ‹•œ“’Ž Œ Š
00000070	86 8c 96 98	8b 66 90 87	82 83 83 83	7a 84 8a cb	†Œ–˜‹f ‡‚ƒƒƒz„ŠË
00000080	5e 5e fb 48	48 82 7c 73	7c 7a 7c 85	7a 5e 73 7c	^^ûHH‚|s|z|…z^s|
00000090	82 99 66 66	74 75 72 61	80 66 6a 73	80 7b 72 4d	‚™fftura€fjs€{rM
000000a0	7d 6e 52 6b	6a 6e 77 63	5f f8 2a 2a	74 68 45 66	}nRkjnwc_ø**thEf
000000b0	66 66 5c 66	74 fc 20 20	55 62 6b 6b	5f 3f e9 22	ff\ftü Ubkk_?é"
000000c0	22 82 4d 4f	55 5d 66 61	56 61 51 5c	6c 55 58 5a	"‚MOU]faVaQ\lUXZ
000000d0	57 55 53 4b	55 62 63 4a	4a 55 51 48	d8 17 17 4a	WUSKUbcJJUQHØ..J
000000e0	52 58 f2 09	09 30 50 86	ff 00 00 43	4b 56 48 4a	RXò..0P†ÿ..CKVHJ
000000f0	48 7b 33 36	e1 04 05 44	45 42 37 45	52 42 41 39	H{36á..DEB7ERBA9
00000100	26 43 78 47	3a 2c 34 3f	49 52 30 31	3a 3a 3c ac	&CxG:,4?IR01::<¬
00000110	09 09 3c 38	35 66 25 28	2f 3a 42 2f	3a 3c 33 33	..<85f%(/:B/:<33
00000120	33 6b 18 19	29 31 41 2a	31 39 34 2f	2a 7a 0f 10	3k..)1A*194/*z..
00000130	29 2d 31 30	2b 28 21 2e	38 33 28 22	29 29 28 21	)-10+(!.83(")")(!
00000140	29 31 27 28	22 22 2a 29	2e 24 20 2a	21 22 20 23	)1'("")*).$ *!" #
00000150	29 2c 1e 17	21 21 21 1b	20 37 21 21	19 28 1c 19	),..!!!. 7!!.(..

History

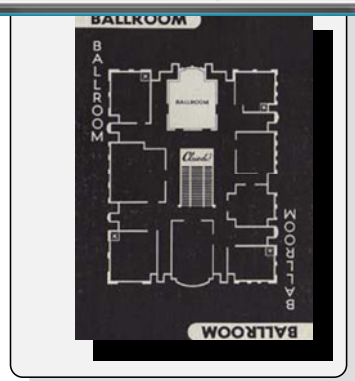
Open

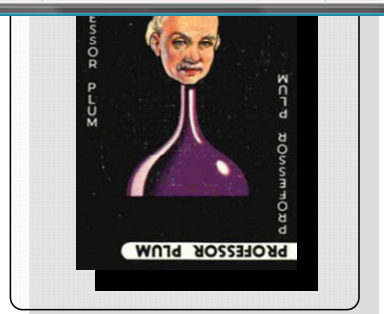
File Attributes

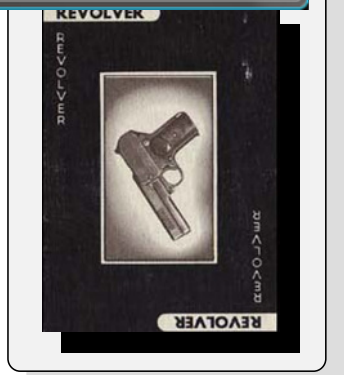
Attribute	Value
File Name	C:\cat01_old.gif
Archive	☑
Hidden	☐
System	☐

Selection | File Attributes

Ready | Offset: 0x00000004 (4) | Size: 0x00000e81 (3,713): 3.63 KB | Hex bytes, 16, Default ANSI | OVR

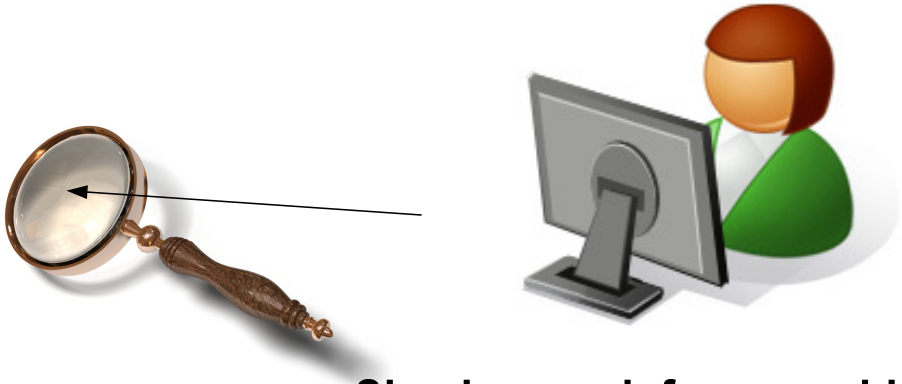






File name changing

File Allocation Table:
1.txt
2.doc
Test.doc
-Delete.gif [deleted]



Simple search for a graphic file will not find the deleted file

Deep scan of the Disk (byte-by-byte)

Obfuscation

Forensic

Author: Prof Bill Buchanan

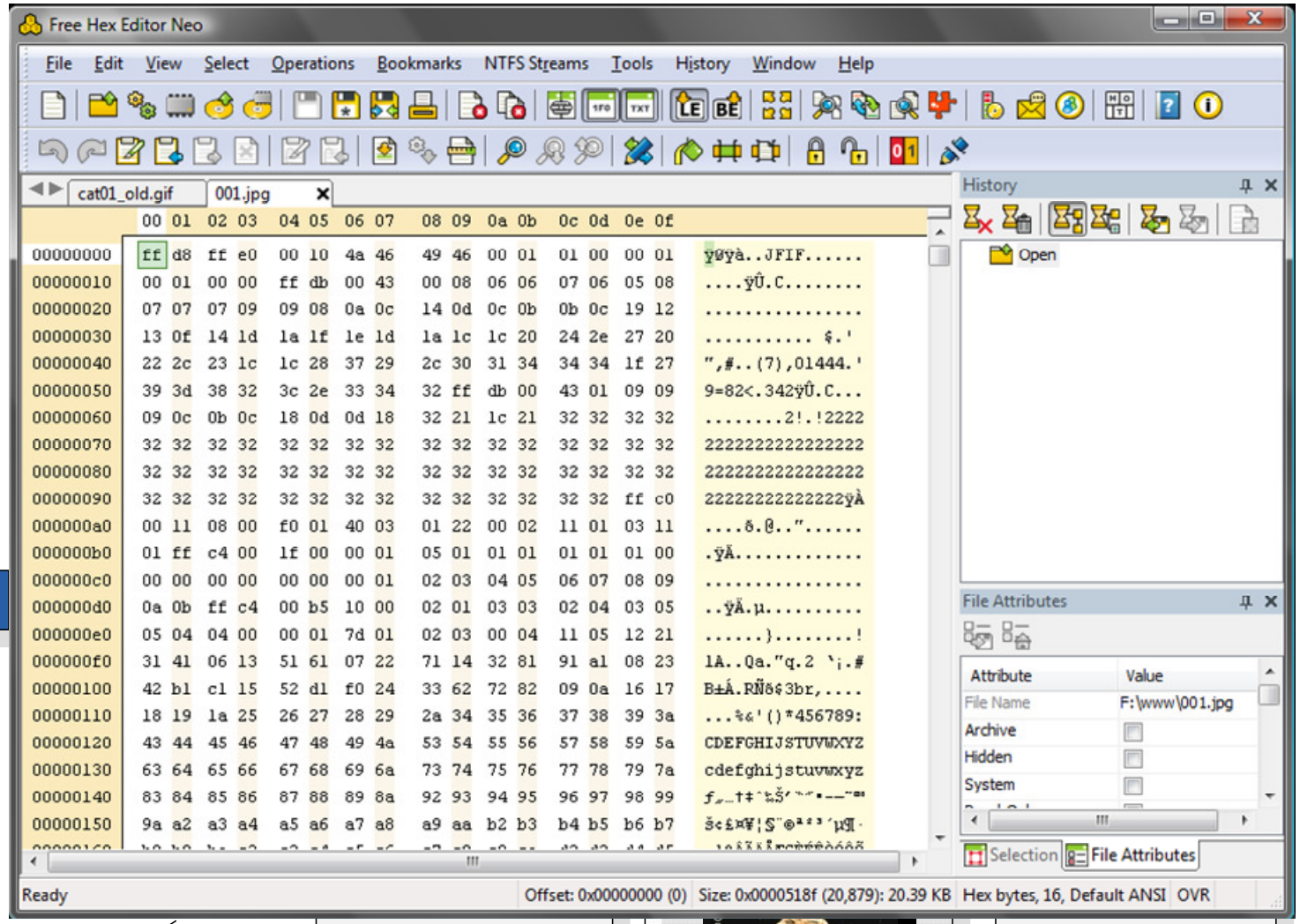
Myphoto.jpg

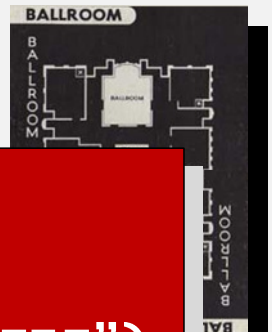
↓

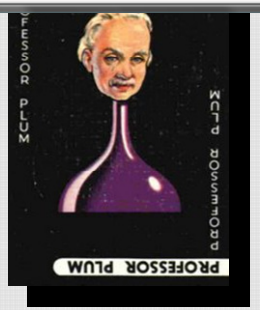
Myphoto.dll

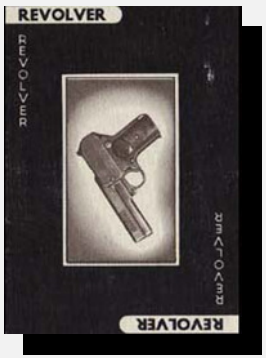
Obfuscation

Forensic







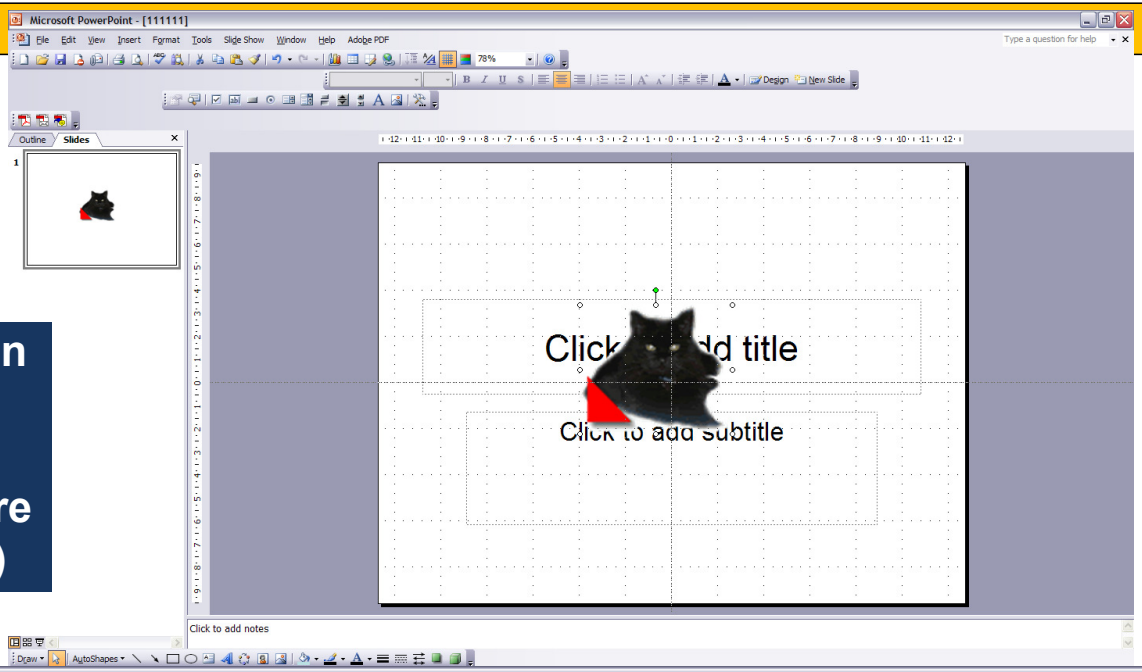


….JFIF...

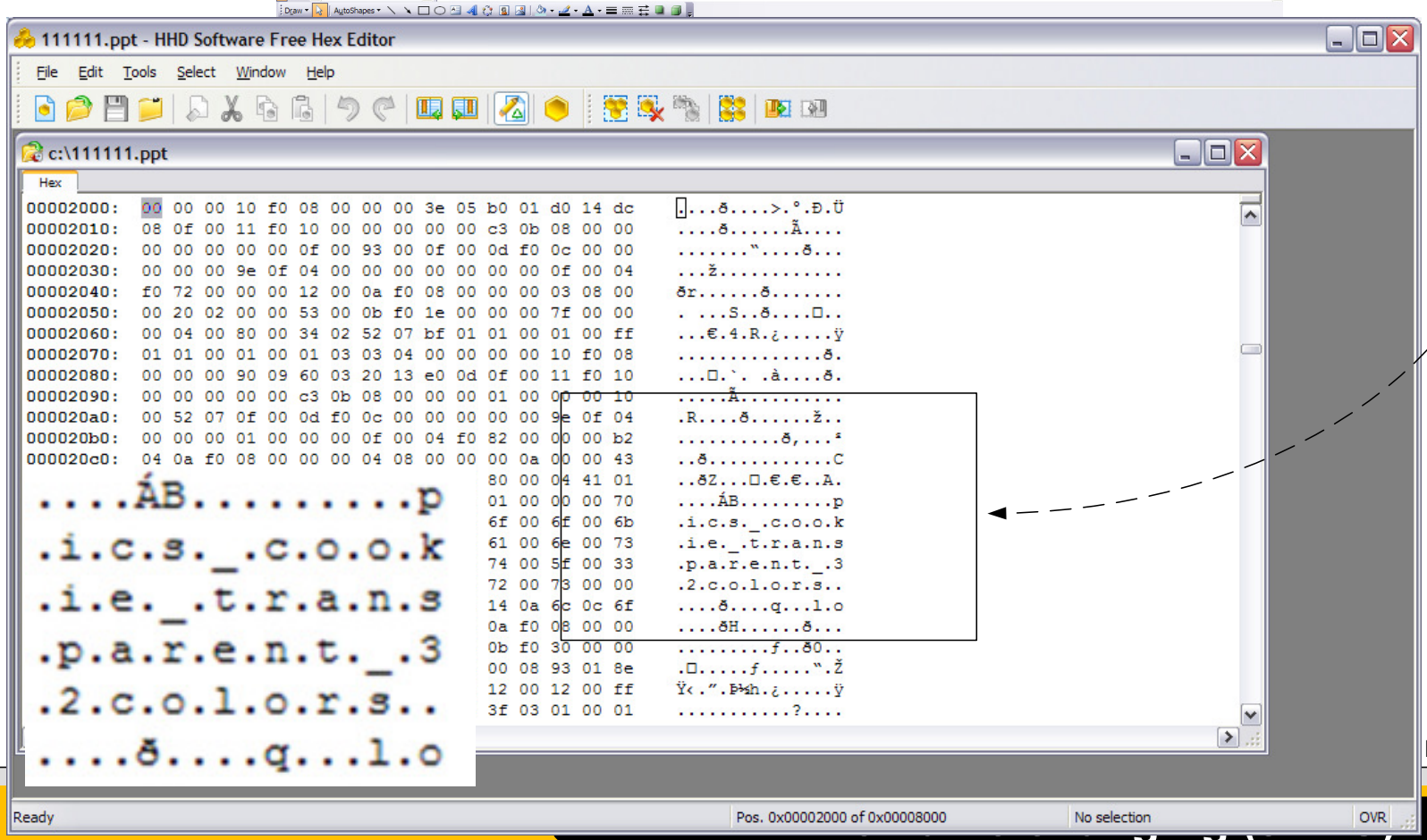
```
Header:   FFD8
Length:   <2 bytes>
Next:     4A,46,49,46,00 ("JFIF")
```

File name changing (JPEG)

Graphic has been imported into PowerPoint (cookie_transparent_32colors.gif)



Meta-data Is still stored in file (but 16-bit character format)



Obfuscation

Forensic

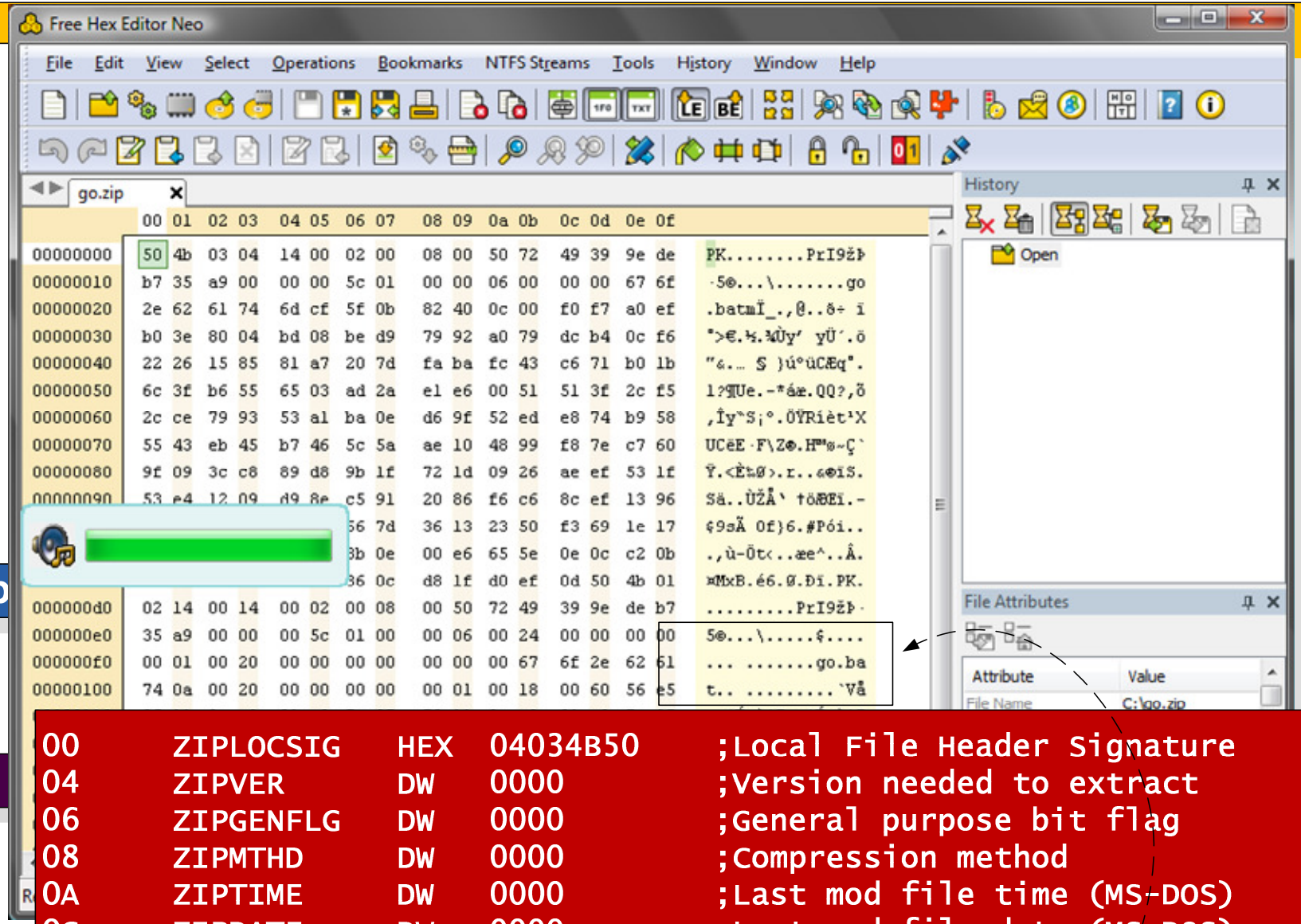
Obfuscation

Forensic

Myzip.zip

↓

Myzip.doc




```
00    ZIPLOCSIG   HEX   04034B50    ;Local File Header Signature
04    ZIPVER      DW    0000       ;Version needed to extract
06    ZIPGENFLG   DW    0000       ;General purpose bit flag
08    ZIPMTHD     DW    0000       ;Compression method
0A    ZIPTIME     DW    0000       ;Last mod file time (MS-DOS)
0C    ZIPDATE     DW    0000       ;Last mod file date (MS-DOS)
0E    ZIPCRC      HEX   00000000   ;CRC-32
12    ZIPSIZE     HEX   00000000   ;Compressed size
16    ZIPUNCMP    HEX   00000000   ;Uncompressed size
1A    ZIPFNLN     DW    0000       ;Filename length
1C    ZIPXTRALN   DW    0000       ;Extra field length
1E    ZIPNAME     DS    ZIPFNLN    ;filename
```

File name changing (ZIP)

Free Hex Editor Neo

File Edit View Select Operations Bookmarks NTFS Streams Tools History Window Help

go.zip pascal.zip

Chap1/chap1_1.pas

Chap1/chap1_2.pas

Chap1/chap1_3.pas

History

Open

File Attributes

Attribute	Value
File Name	F:\www\zips\pascal
Archive	
Hidden	
System	
Read-Only	
Sparse	

Selection File Attributes

Ready Offset: 0x000000b9 (185) Size: 0x0000bdcf (48,591): 47.45 KB Hex bytes, 16, Default ANSI OVR

Myzip.z

Myzip.do

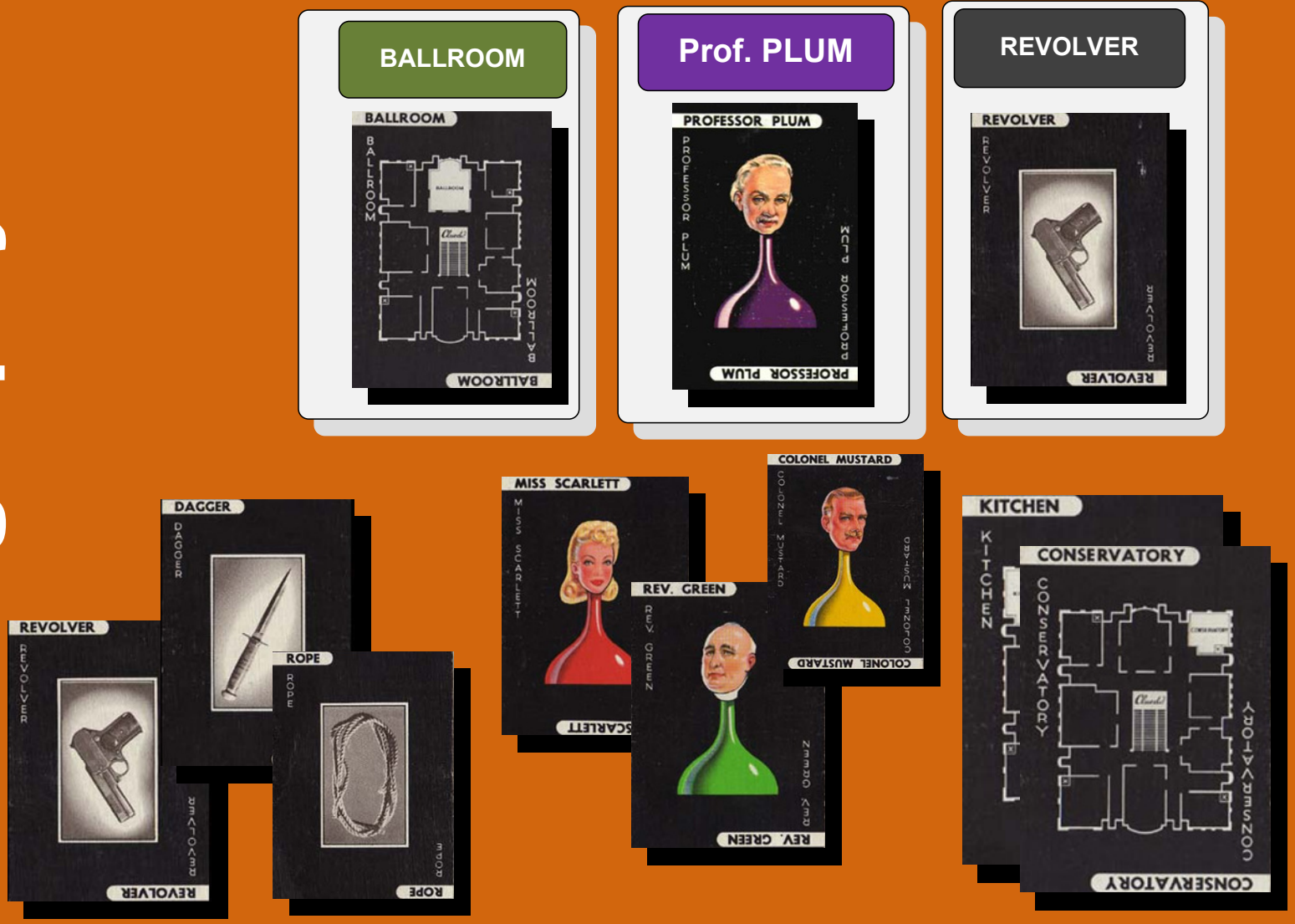
Prof. P

Obfuscation

Forensic

File name changing (ZIP)

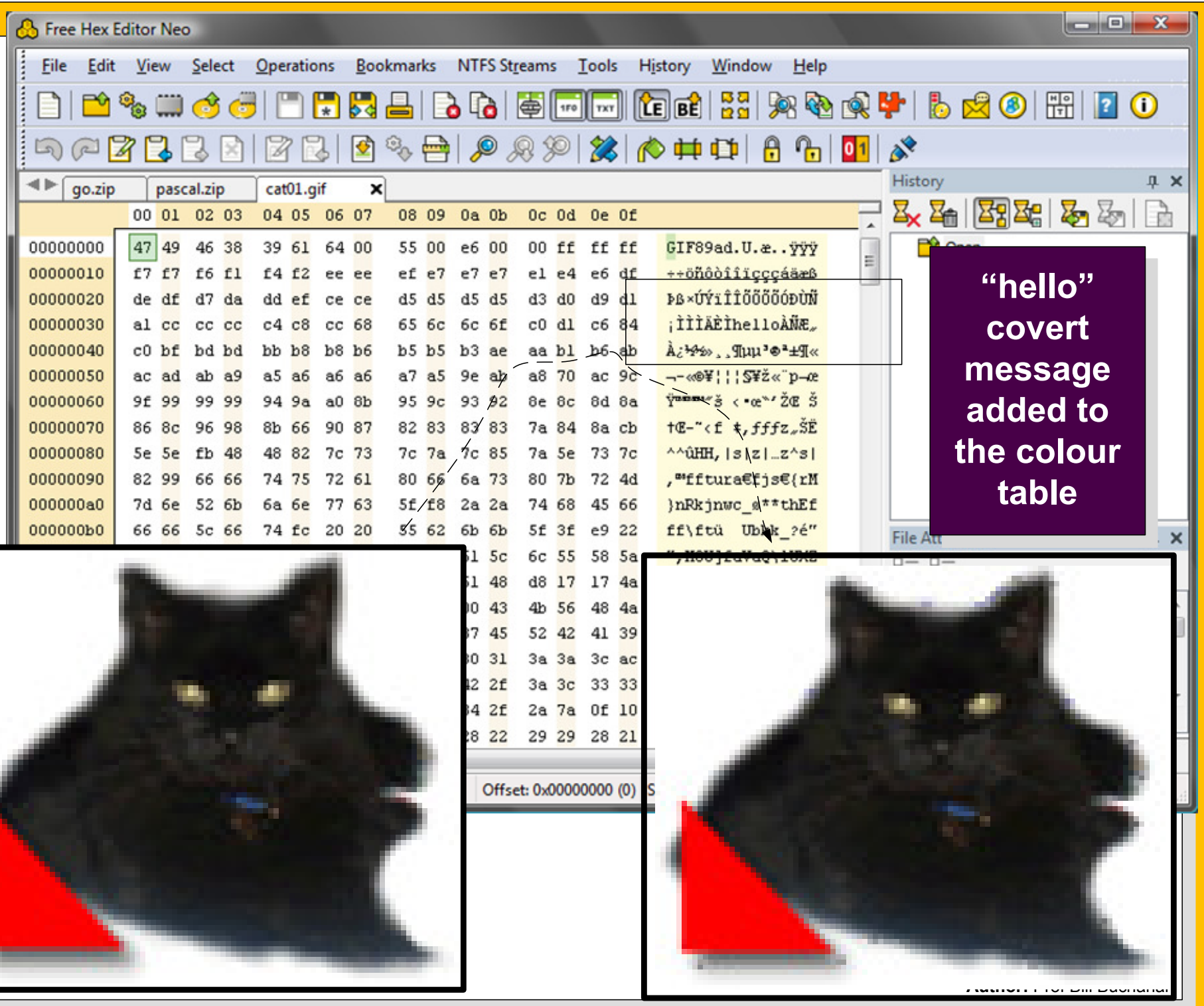
Stenography



Author: Prof Bill Buchanan

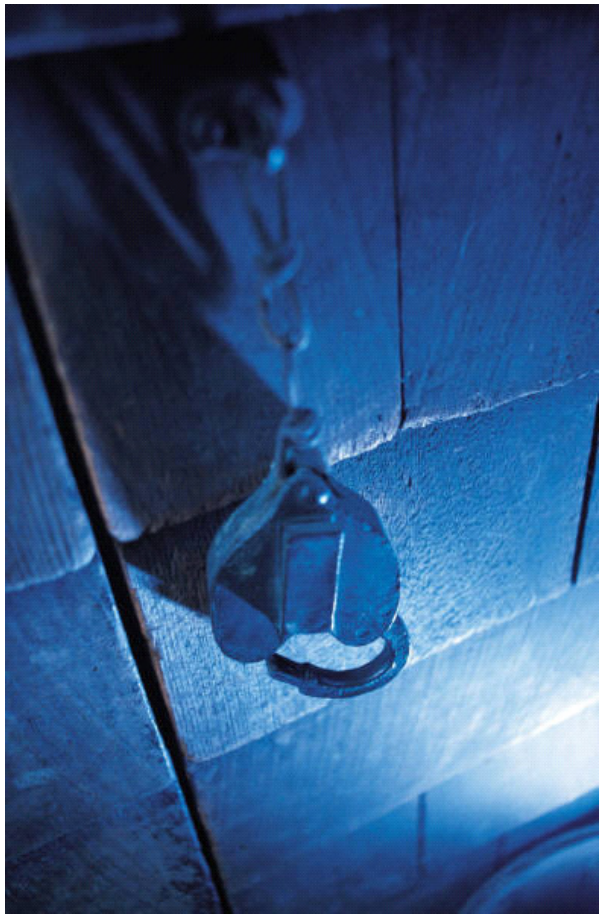
Stenography

Forensic



"hello" covert message added to the colour table

Covert messages (in a GIF file)



Hello how are you?

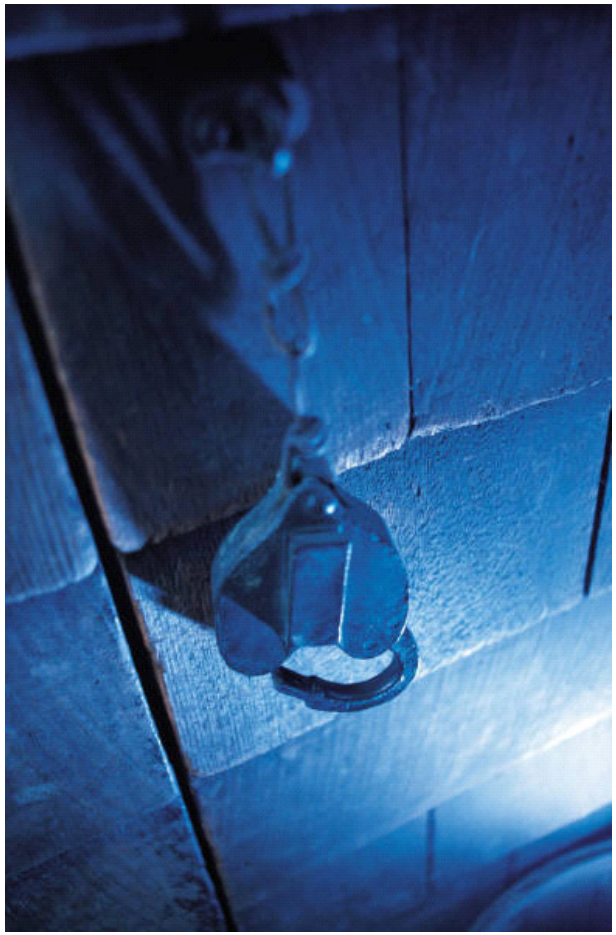
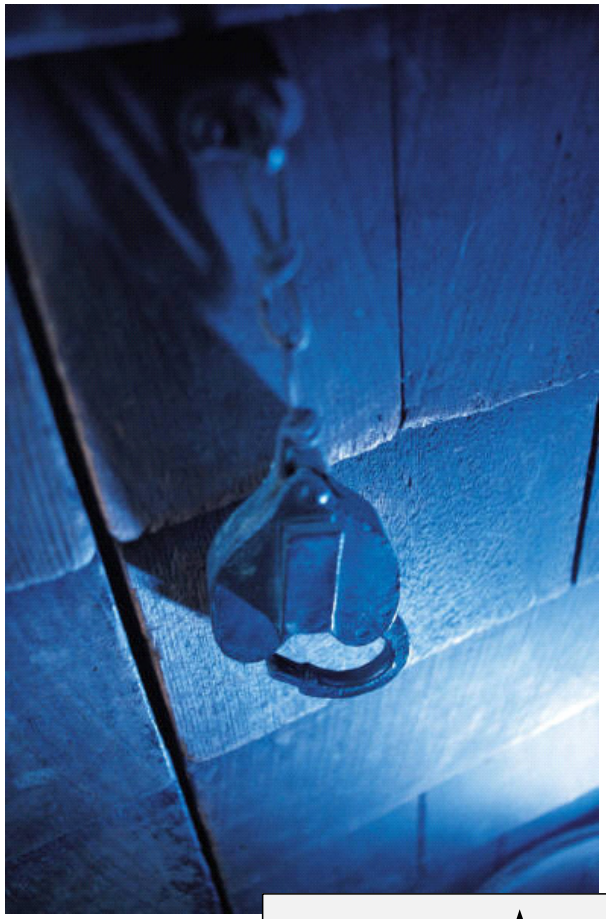


Image does not change as text is hidden in the JPEG conversion

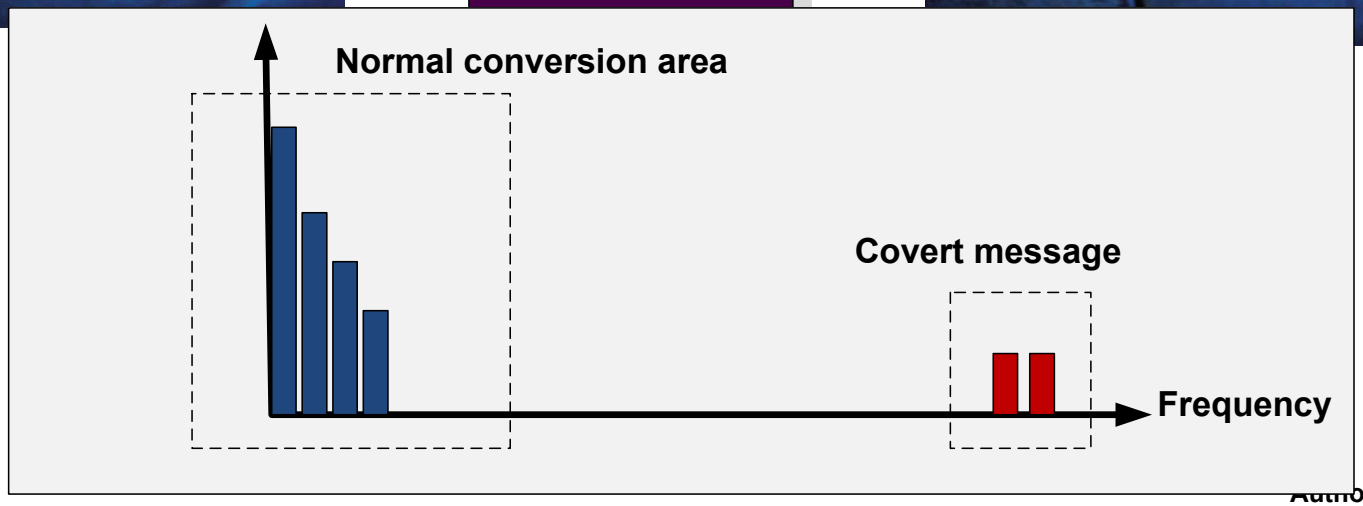
Author: Prof Bill Buchanan

Stenography

Forensic



Hello how are you?



Author: Prof Bill Buchanan

Stenography involves hiding information in the body of the content

Stenography

Forensic

Original image

Image+Message

Changes that are made are small and cannot be picked-up by the human eye, unless the image is zoomed-in

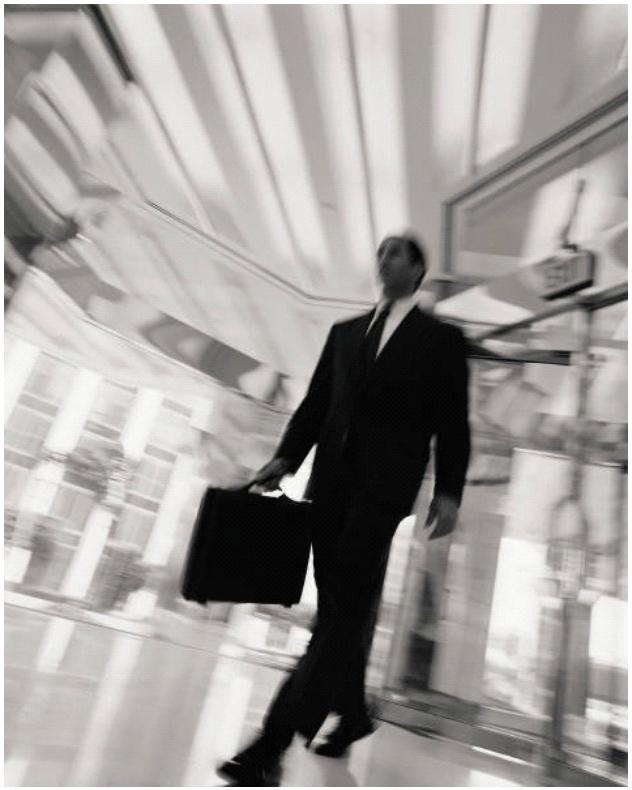
Author: Prof Bill Buchanan

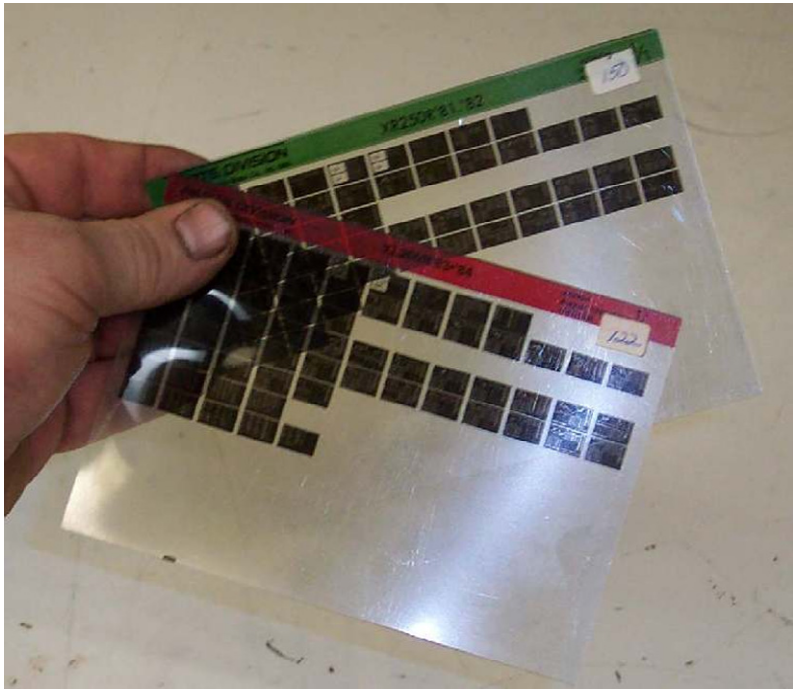
Covert Channels

Author: Prof Bill Buchanan

Covert channels have been used by secret operations for a long time, such as:

- Passing a briefcase in a busy place.
- Hiding microfilms in objects.
- Using templates for typewritten text





Author: Prof Bill Buchanan

Let everyone tango. This has Edward's mind in some simple inquiry of nothing, before everyone gets into Nirvana.

Author: Prof Bill Buchanan

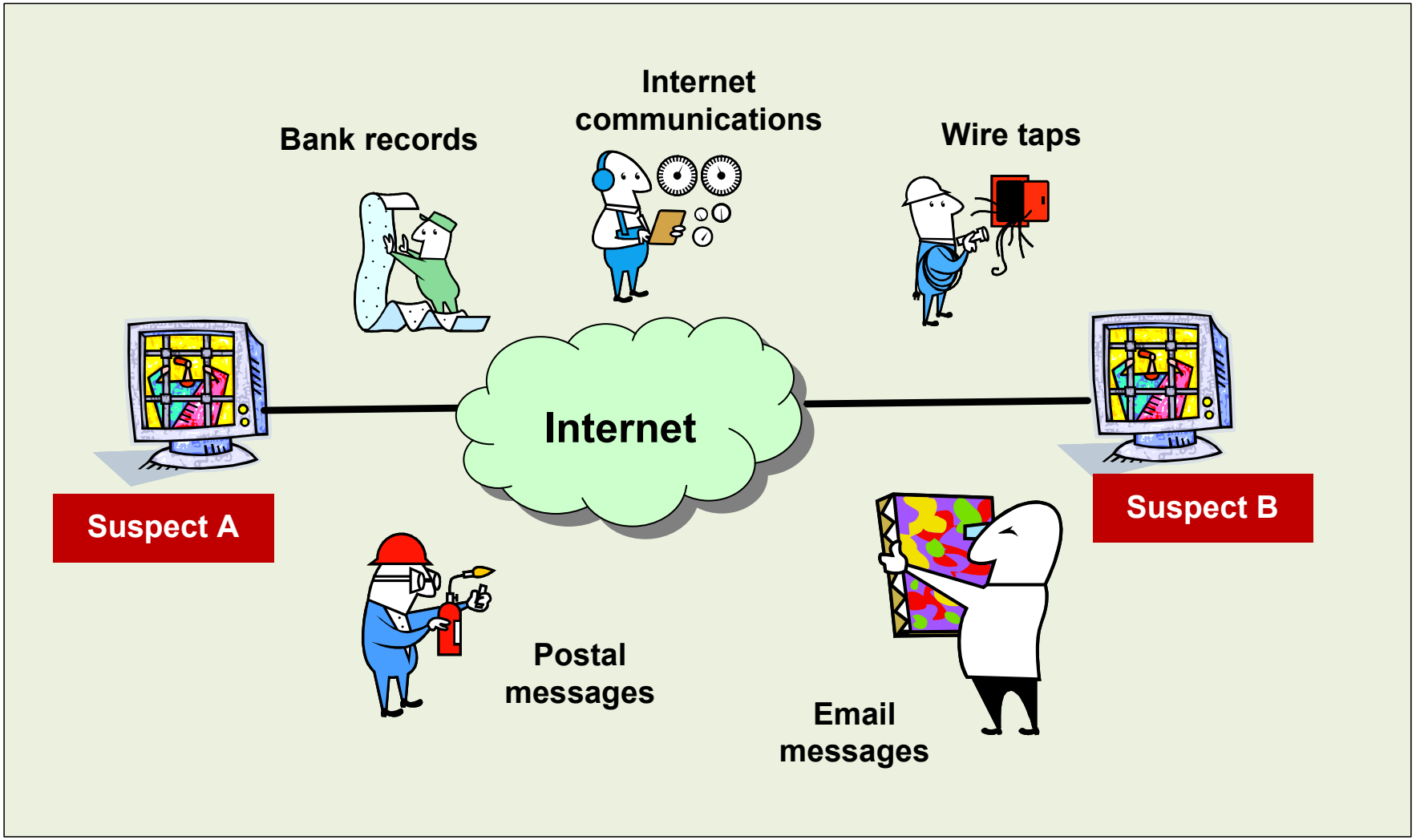
Covert Channels

Forensic

Let everyone tango. This has Edward's mind in some simple inquiry of nothing, before everyone gets into Nirvana.

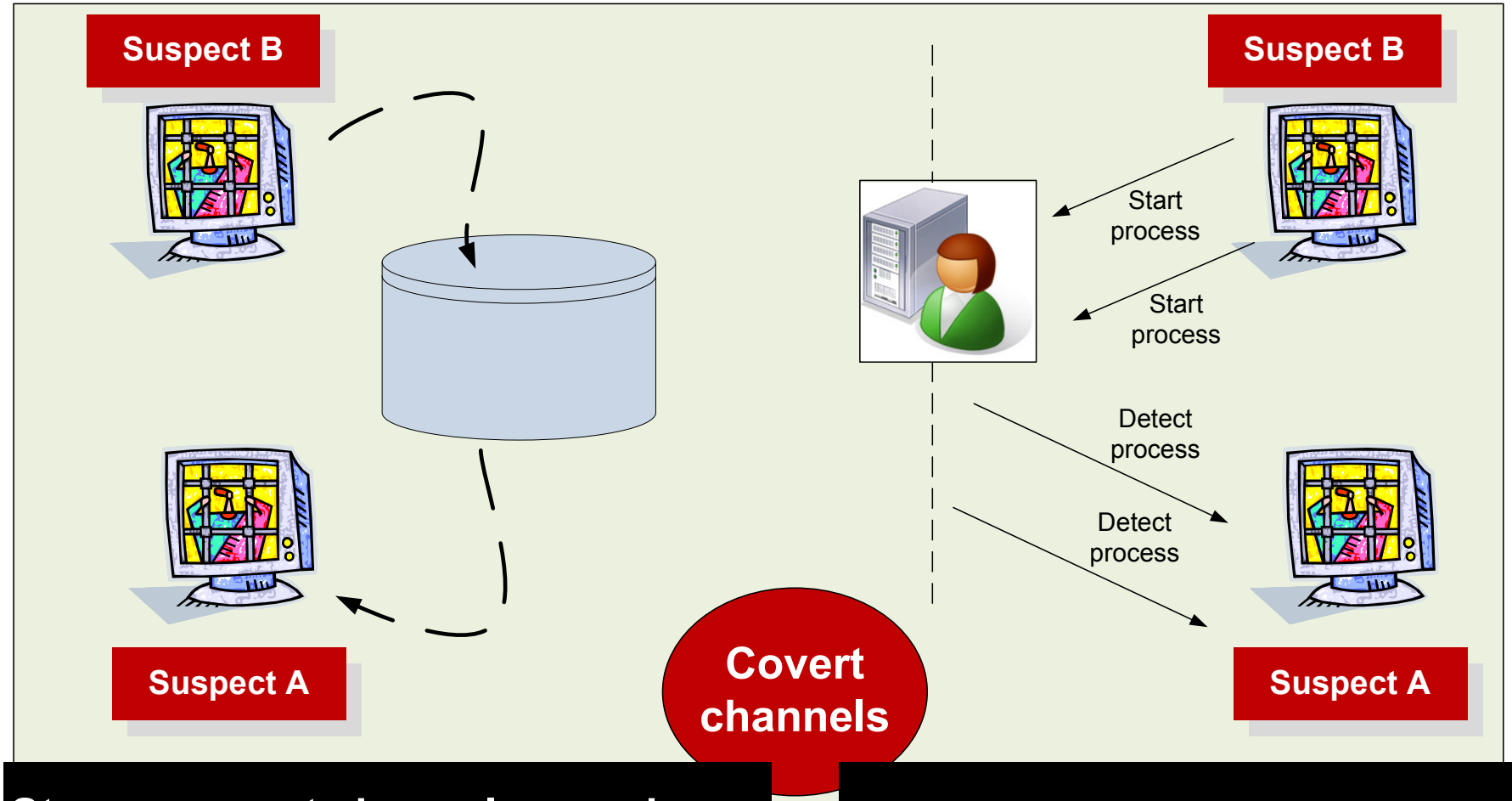
Let the mission begin

Author: Prof Bill Buchanan



A covert channel is typically used when the suspects know that they are being monitored

Author: Prof Bill Buchanan

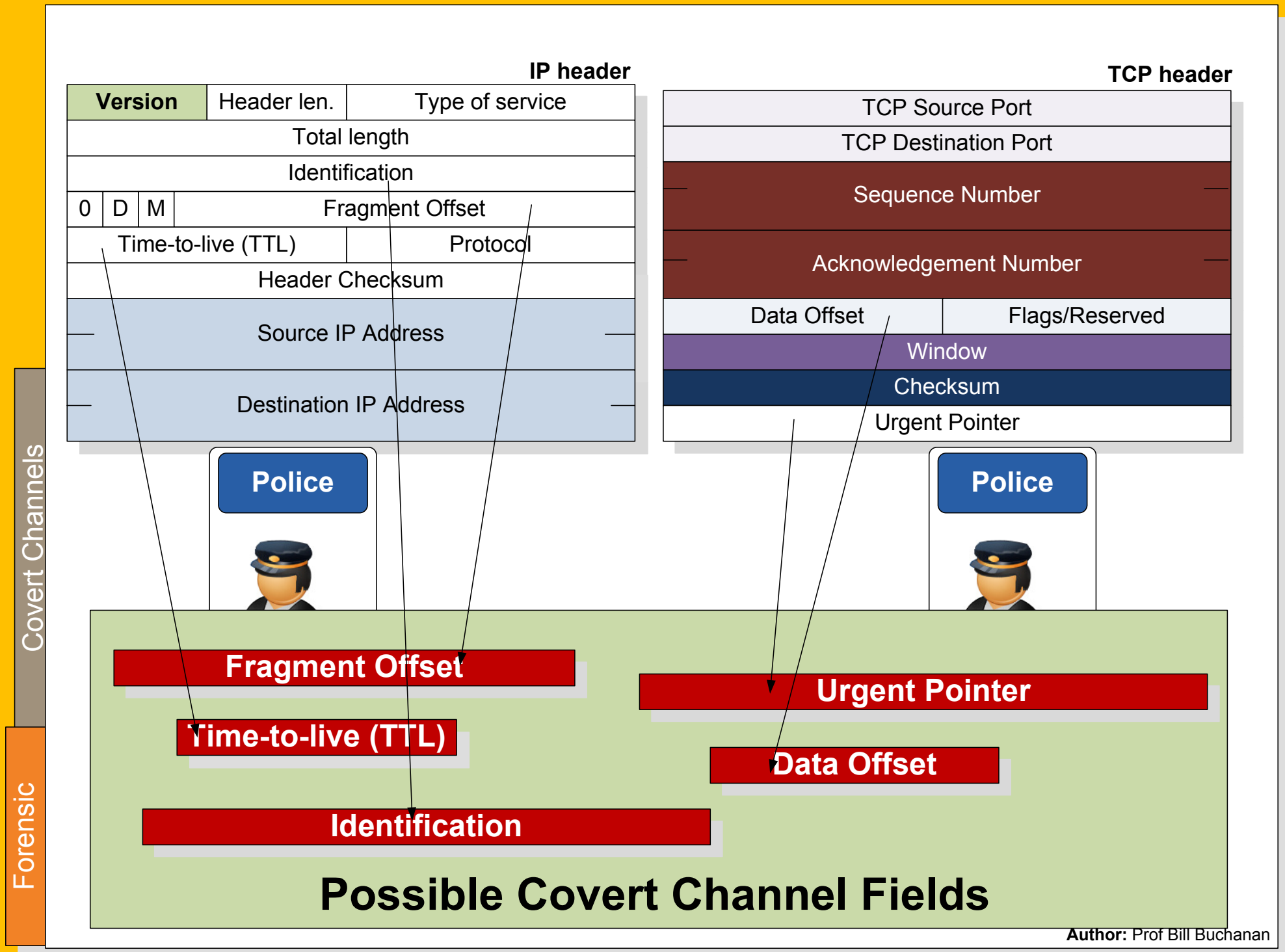


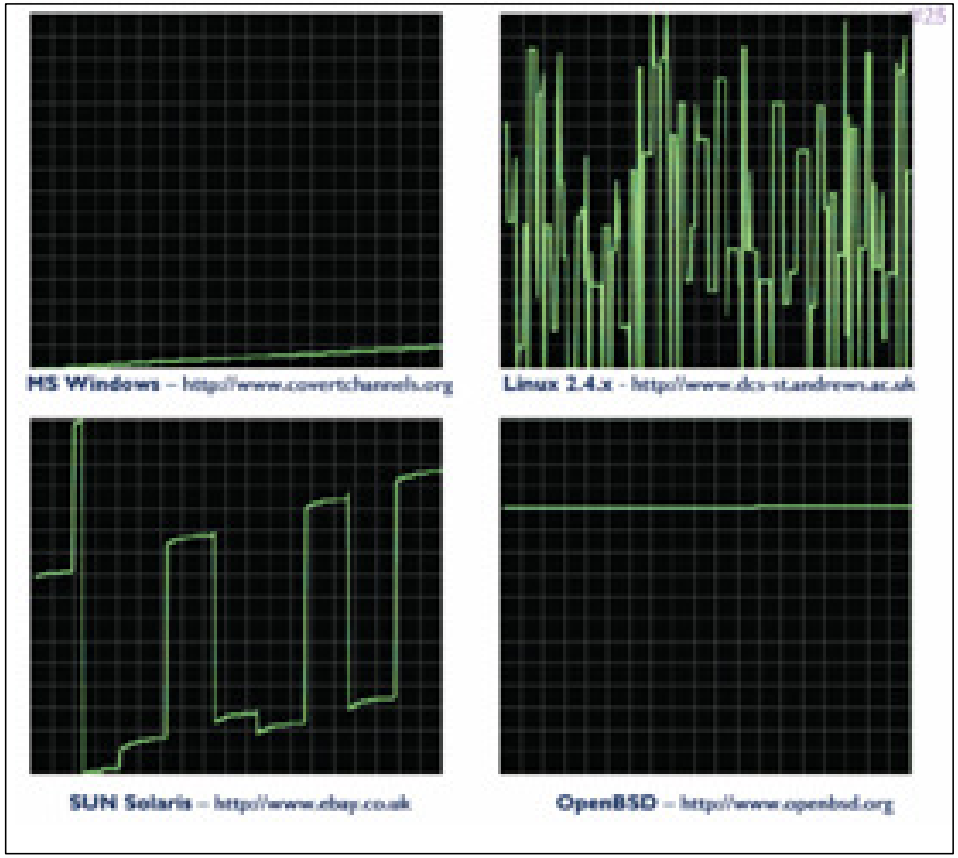
Storage covert channels are where one process uses direct (or indirect) data writing, whilst another process reads the data. It generally uses a finite system resource that is shared between entities with different privileges.

Covert timing channels use the modulation of certain resources, such as the CPU timing, in order to exchange information between processes.

IP and TCP Covert Channels

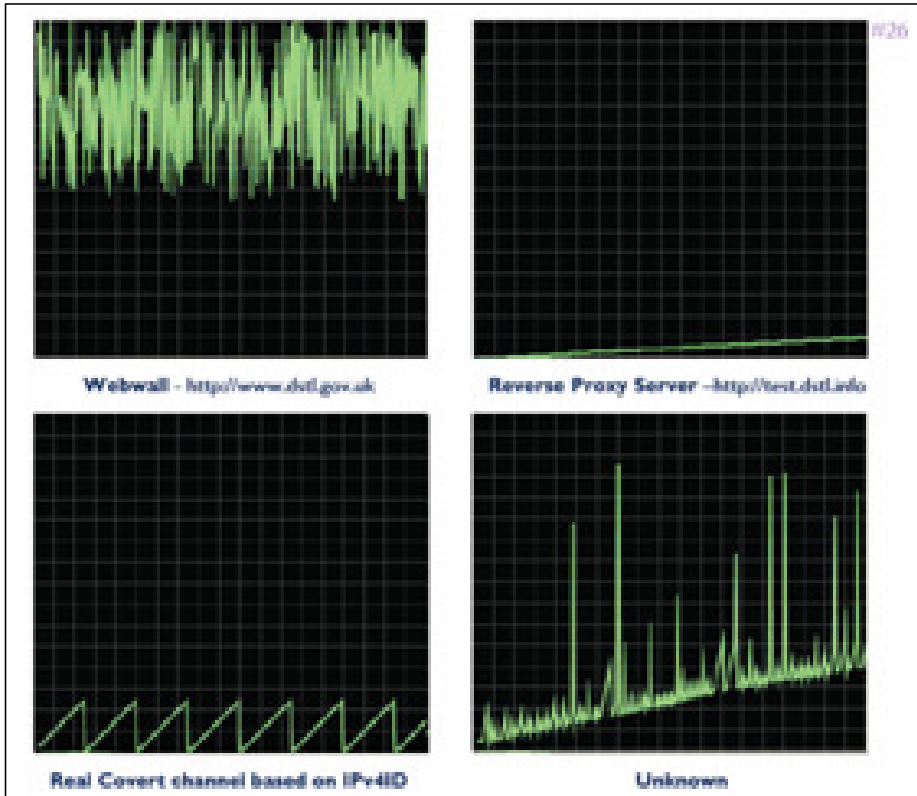
Author: Prof Bill Buchanan


IP header
Version
Header len.
Type of service
Total length
Identification
0
D
M
Fragment Offset
Time-to-live (TTL)
Protocol
Header Checksum
Source IP Address
Destination IP Address
TCP header
TCP Source Port
TCP Destination Port
Sequence Number
Acknowledgement Number
Data Offset
Flags/Reserved
Window
Checksum
Urgent Pointer
Police
Police
Covert Channels
Forensic
Fragment Offset
Time-to-live (TTL)
Identification
Urgent Pointer
Data Offset
Possible Covert Channel Fields
Author: Prof Bill Buchanan



Version	Header len.	Type of service
Total length		
Identification		
0 D M	Fragment Offset	
Time-to-live (TTL)		Protocol
Header Checksum		
Source IP Address		
Destination IP Address		

IP Header.
IPv4 ID: This field is an identification field and is primarily used for uniquely identifying fragments of an original IP
Source: David Llamas



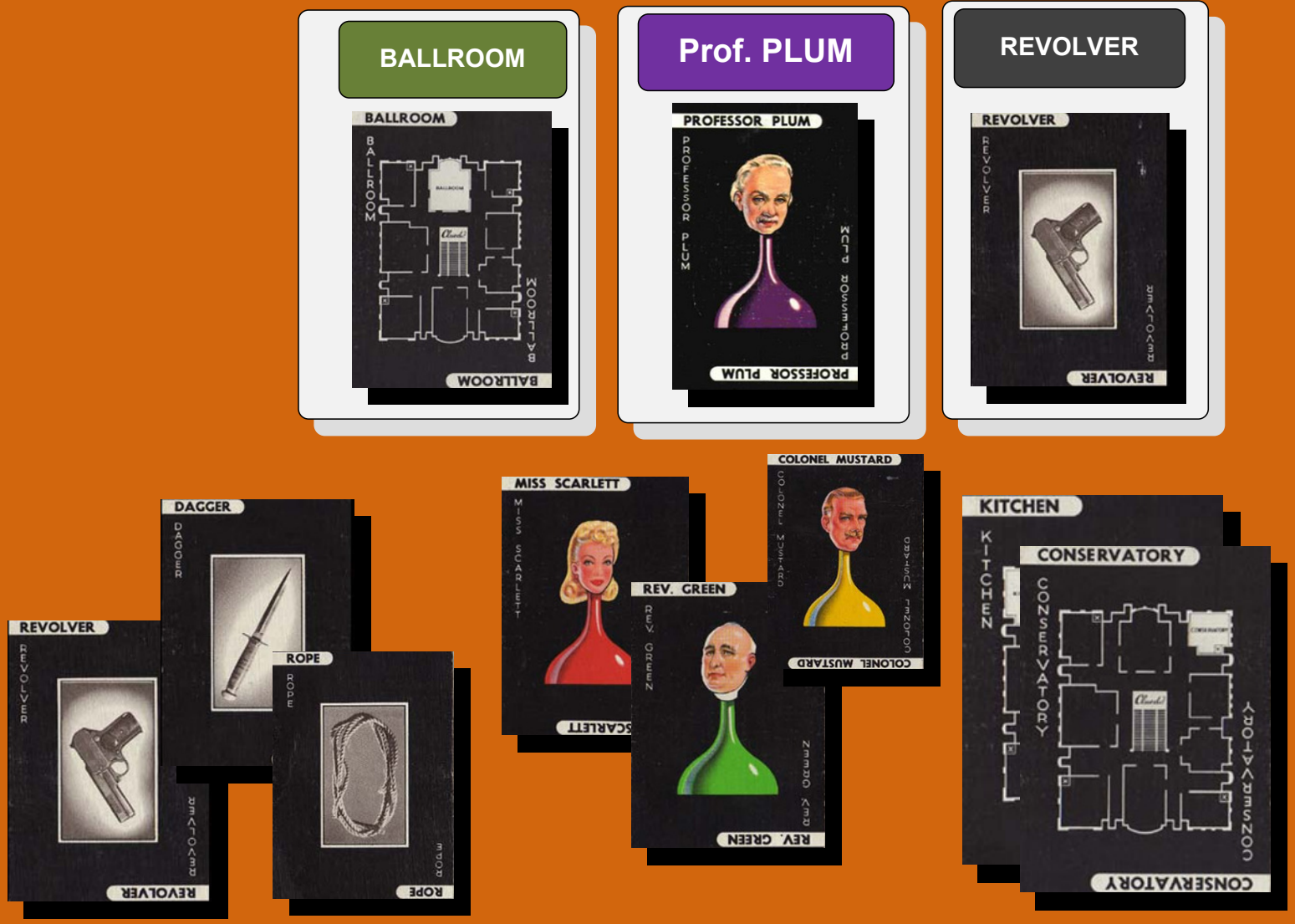
Author: Prof Bill Buchanan

Covert Channels

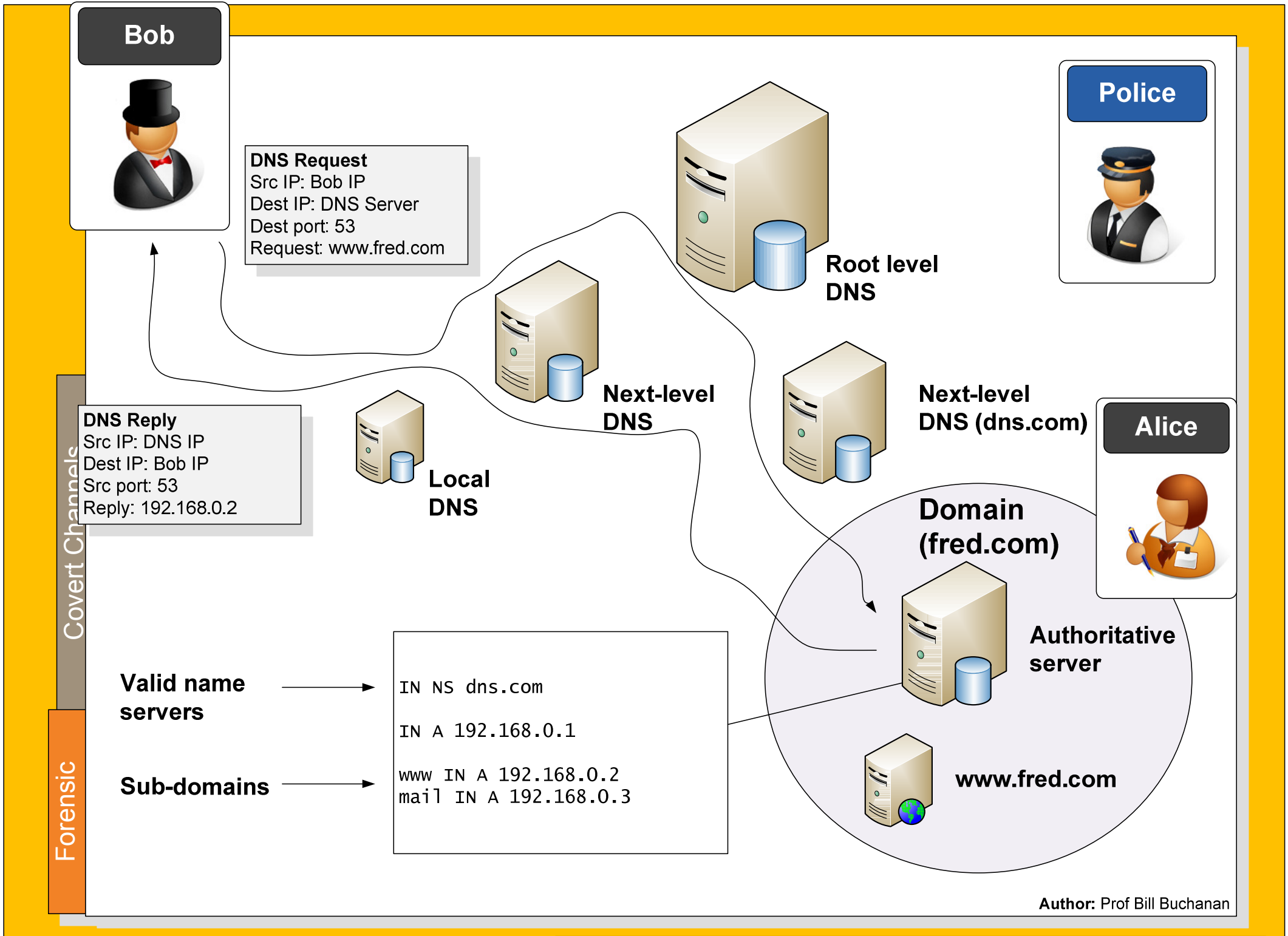
Forensic

IPv4 ID Field

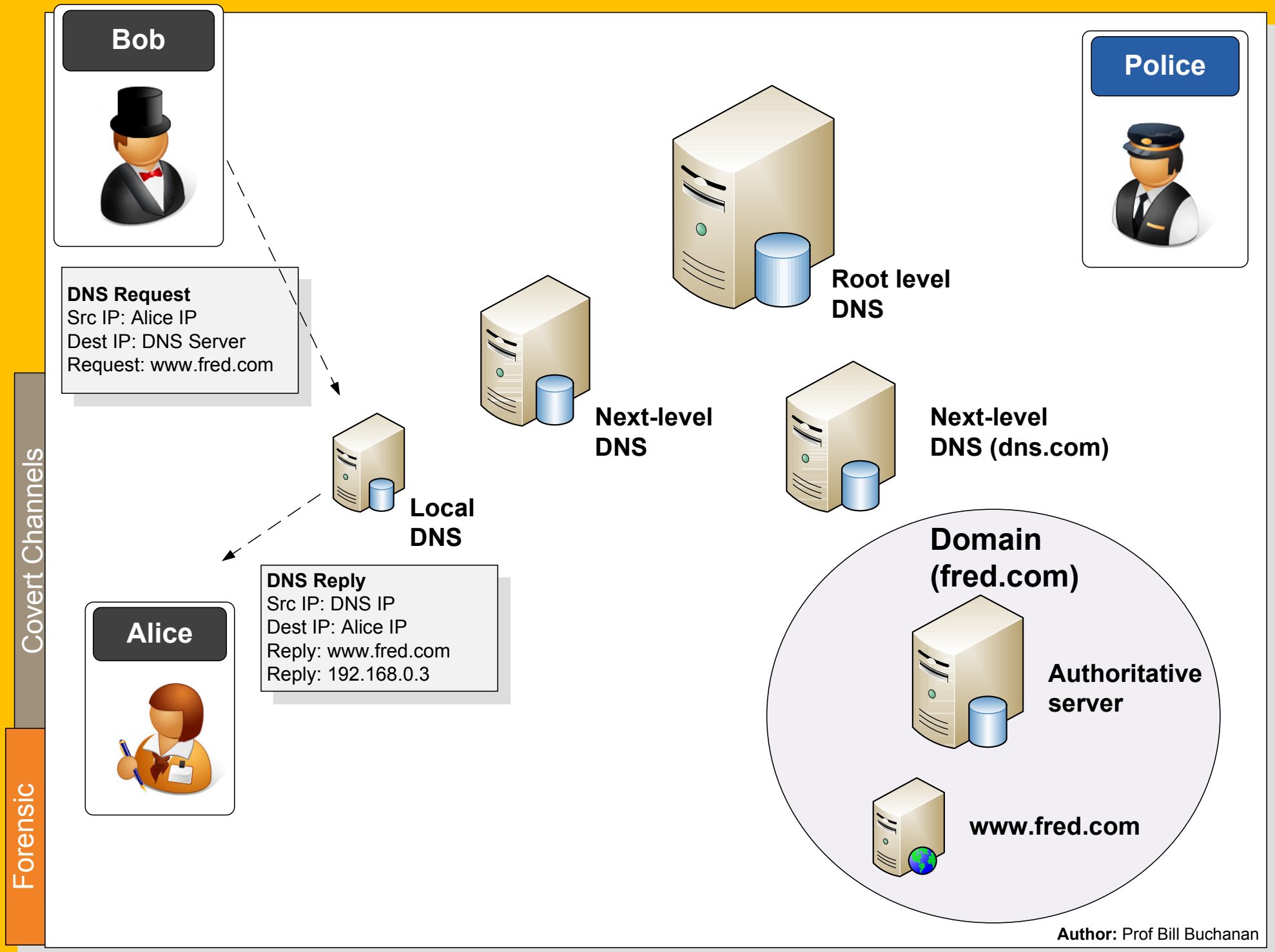
DNS Covert Channels



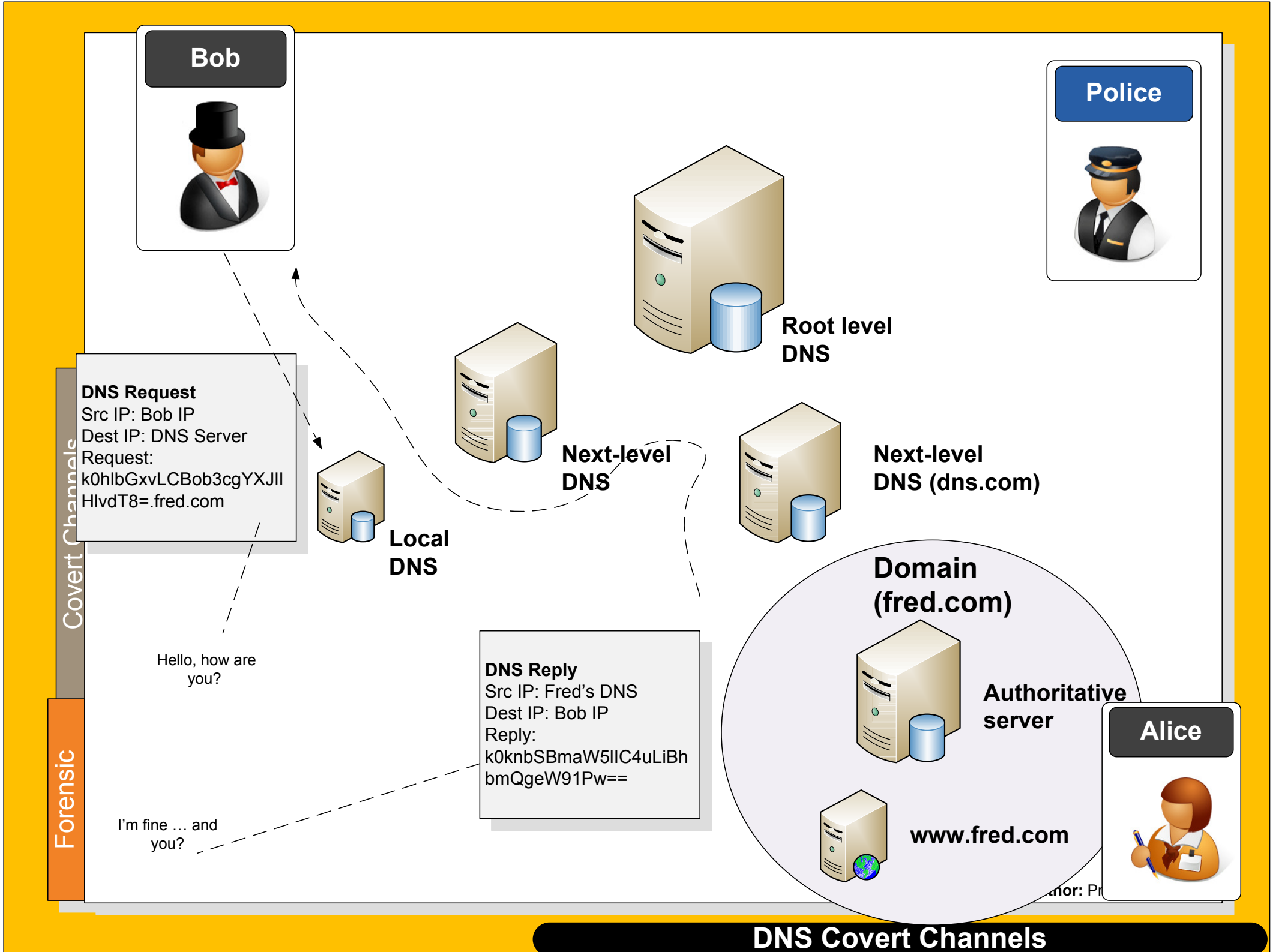
Author: Prof Bill Buchanan



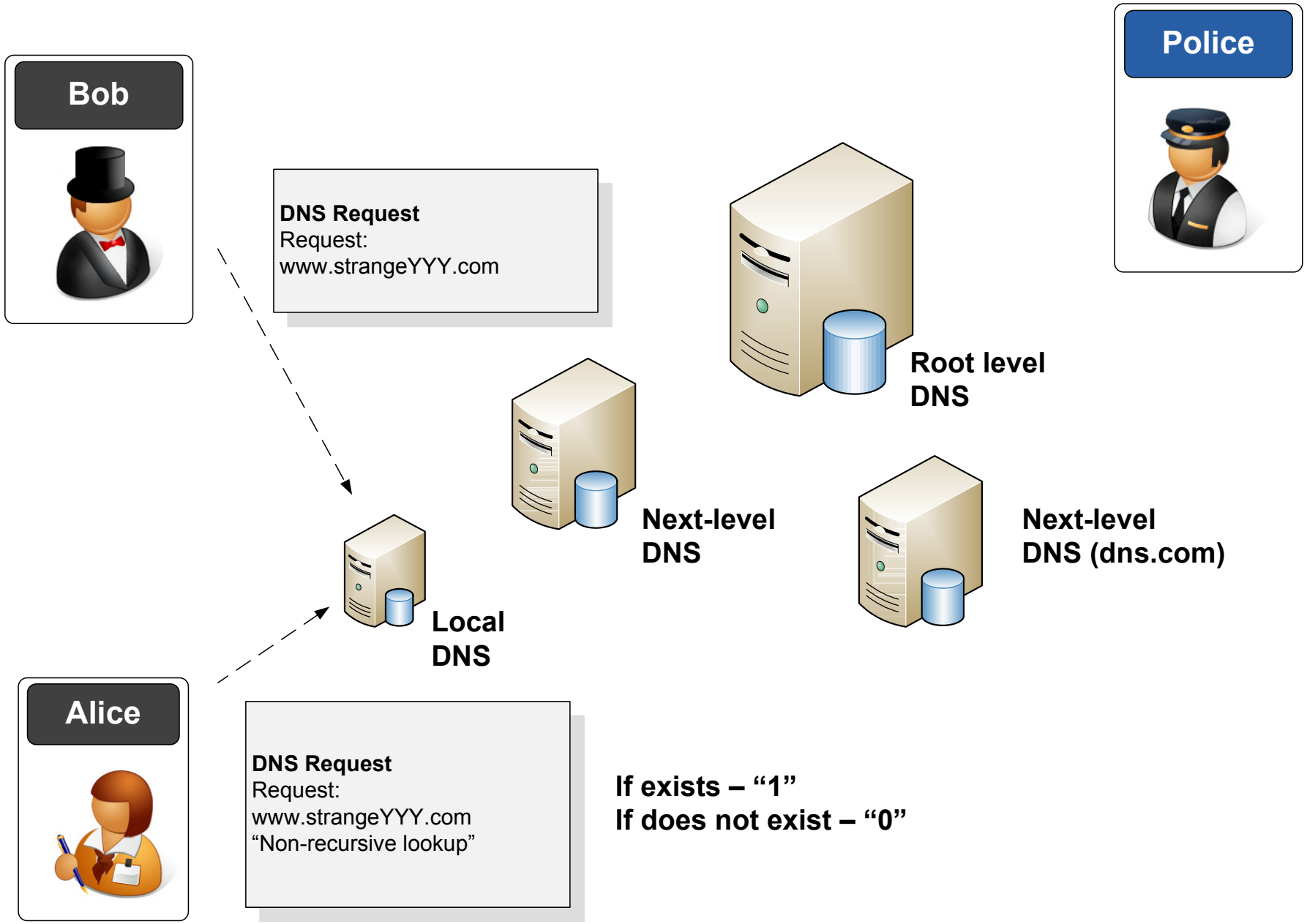
DNS Covert Channels



DNS Covert Channels



DNS Covert Channels



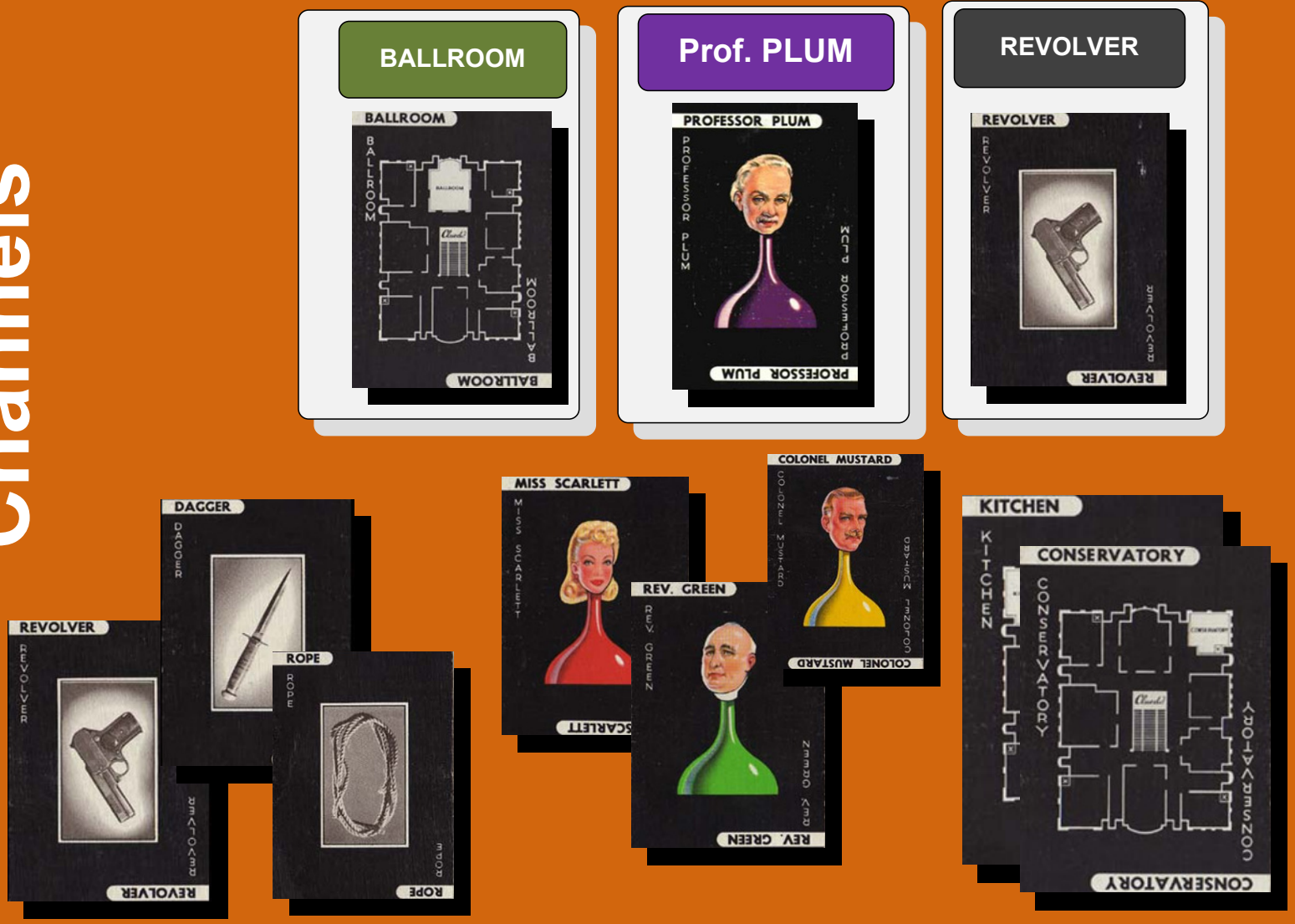
Covert Channels

Forensic

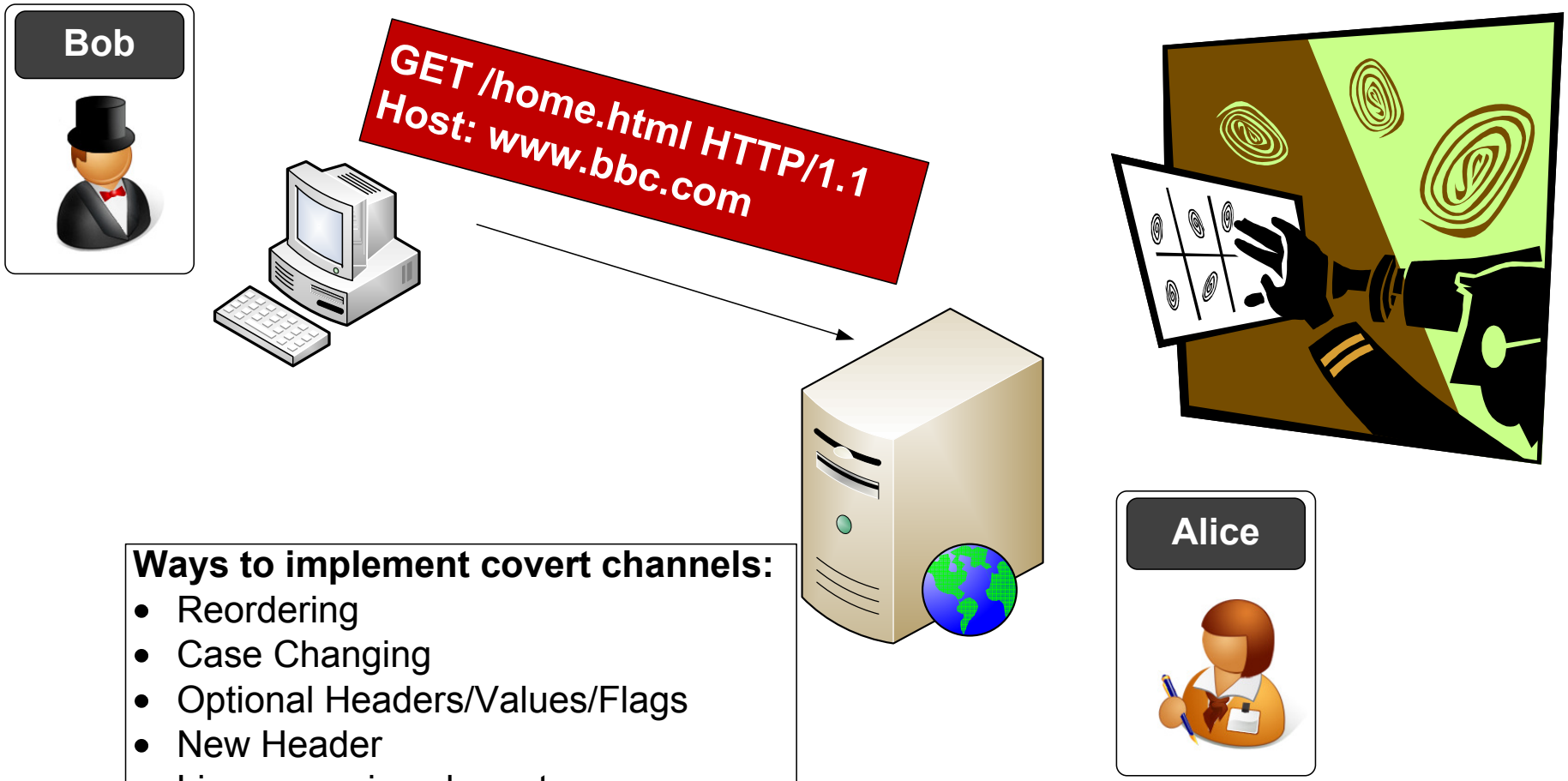
Author: Prof Bill Buchanan

DNS Covert Channels (Timing)

HTTP Covert Channels



Author: Prof Bill Buchanan



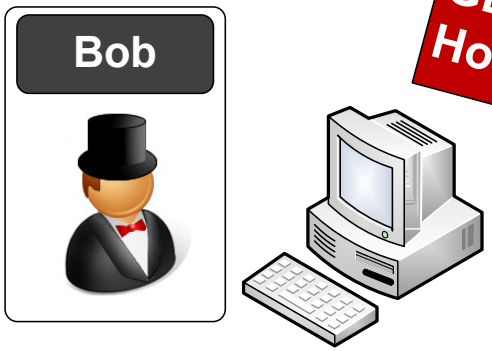
Ways to implement covert channels:

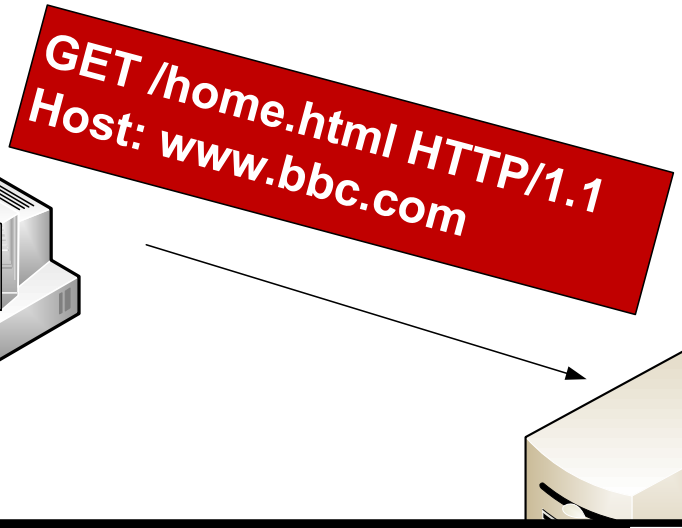
- Reordering
- Case Changing
- Optional Headers/Values/Flags
- New Header
- Linear spacing characters
- Modifying server object

Detection:

- Protocol-based
- Signature-based
- Behaviour-based

Author: Prof Bill Buchanan





Covert Channels

1st request

```
GET / HTTP/1.1
Accept: */*
Accept-Language: en-gb
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0)
Host: www.bbc.com
Connection: Keep-Alive
```

Transmission: '0'

Forensic

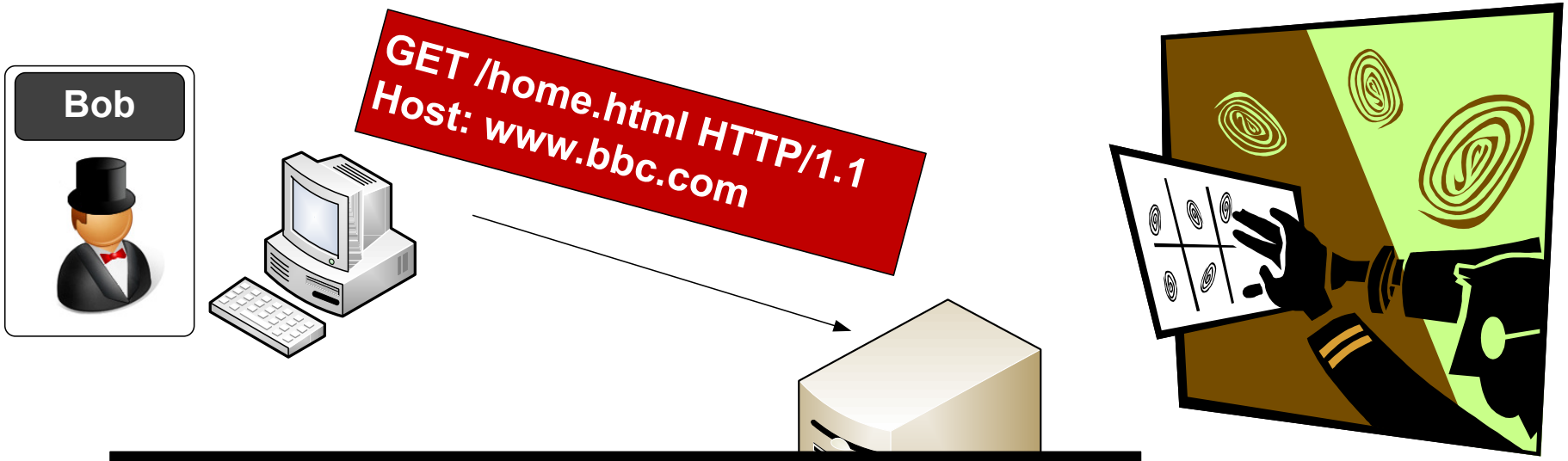
2nd request

```
GET / HTTP/1.1
Accept: */*
Accept-Language: en-gb
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0)
Connection: Keep-Alive
Host: www.bbc.com
```

Transmission:'1'

Author: Prof Bill Buchanan

HTTP Covert Channel (Re-ordering)

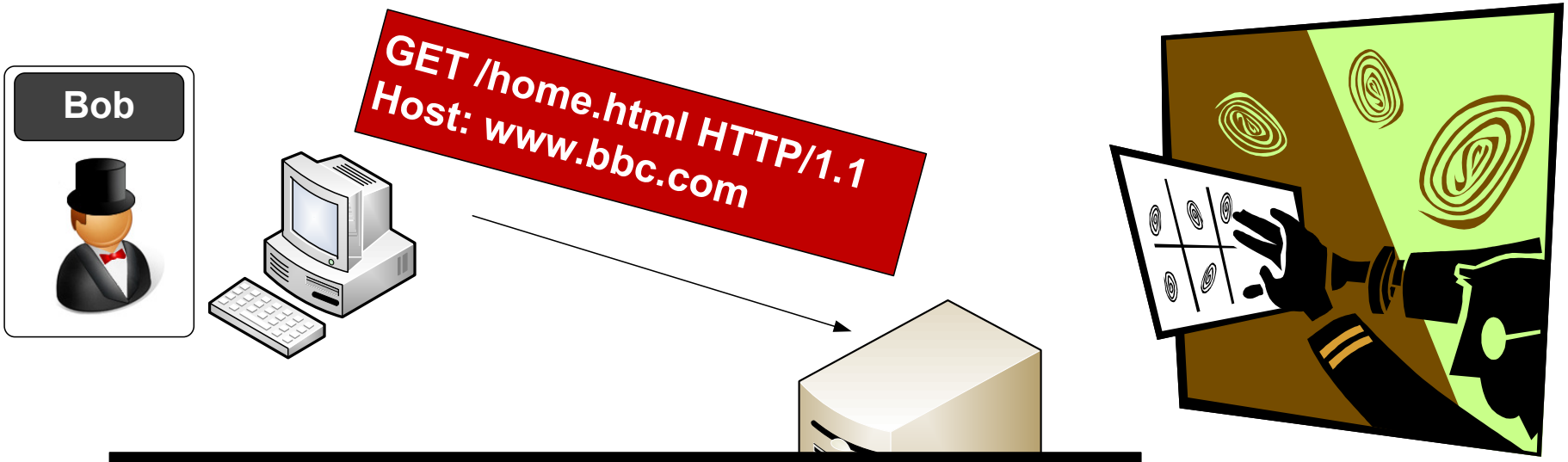



```
GET / HTTP/1.1
Accept: */*
Accept-Language: en-gb
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0)
Host: www.bbc.com
ConnECtIon: Keep-Alive
```

0x72 -"R"

Author: Prof Bill Buchanan

HTTP Covert Channel (Changing case)



Covert Channels

1st request

```
GET / HTTP/1.1
Accept: */*
Accept-Language: en-gb
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0)
Host: www.bbc.com
Connection: Keep-Alive
```

Transmission: '0'

Forensic

2nd request

```
GET / HTTP/1.1
Accept: text/xml, */*;q=0.5
Accept-Language: en-gb
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0)
Host: www.bbc.com
Connection: Keep-Alive
```

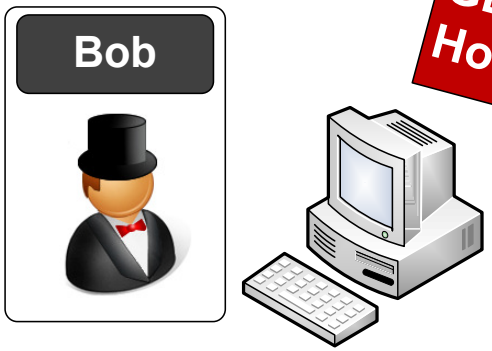
Transmission: '1'

Author: Prof Bill Buchanan

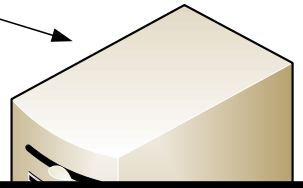
HTTP Covert Channel (Optional flags/fields)

Author: Prof Bill Buchanan

HTTP Covert Channel (New field)



GET /home.html HTTP/1.1
Host: www.bbc.com



Covert Channels

```
GET / HTTP/1.1
Accept: */*
Accept-Language: en-gb
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0
Host: www.bbc.com
Connection: Keep-Alive
```

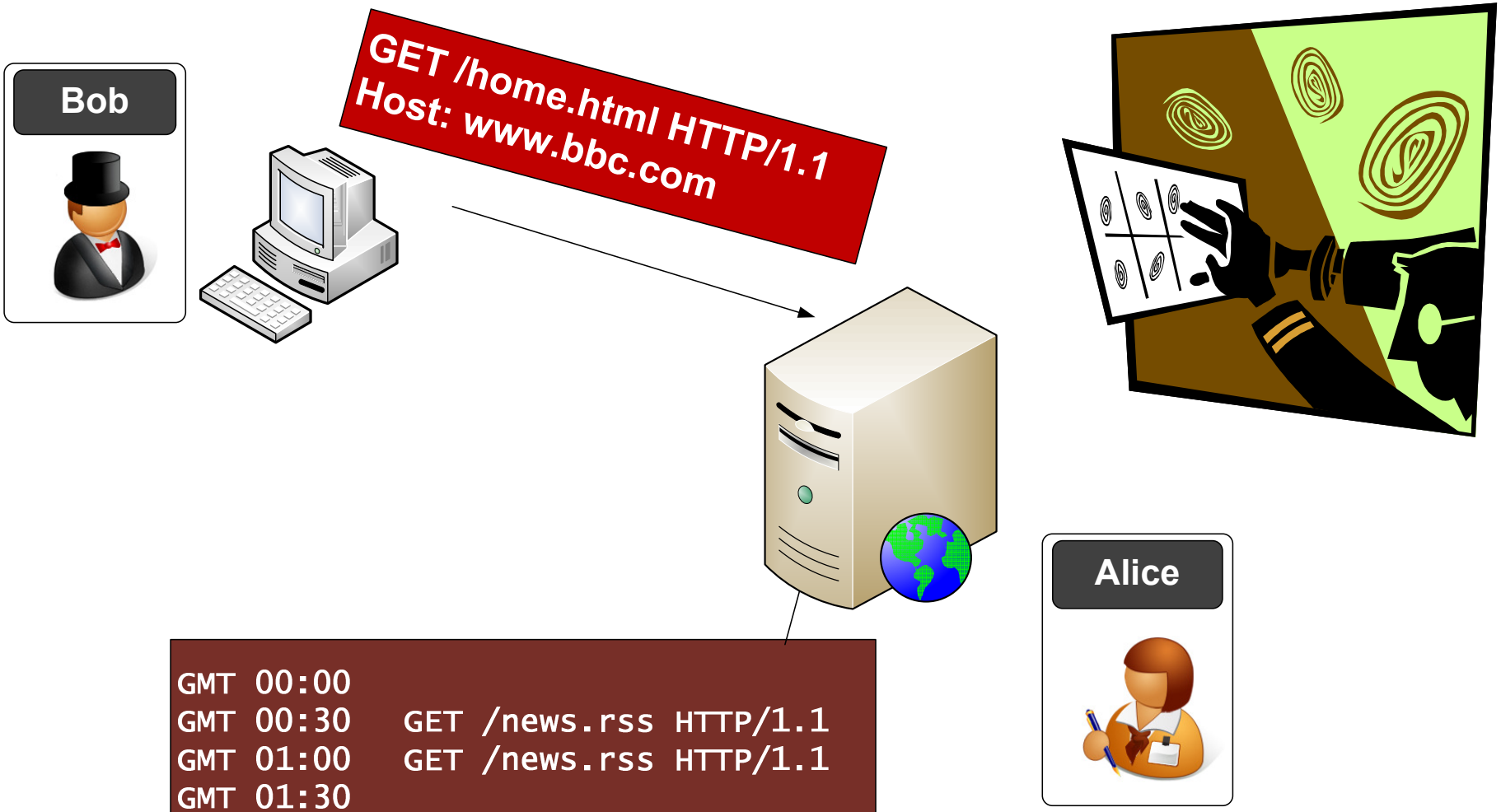
Forensic

```
GET[SP]/[SP]HTTP/1.1[CRLF]
Accept:[SP]*/*[HT][SP][SP][HT][SP][SP][SP][CRLF]
Accept-Language:[SP]en-gb[CRLF]
Accept-Encoding:[SP]gzip,[SP]deflate[CRLF]
User-Agent:[SP]Mozilla/4.0[CRLF]
Host:[SP]www.bbc.com[CRLF]
Connection:[SP]Keep-Alive[CRLF]
```

```
[SP]    SPACE - 0
[HT]    TAB - 1
[CRLF]  CR + LF

01001000 = "H"
```


HTTP Covert Channel (Spacing characters)



Author: Prof Bill Buchanan

HTTP Covert Channel (Timing channel)

Analysis

Author: Prof Bill Buchanan

Investigation

ICMP activity

DNS activity

TCP flags

Application Protocol activity

ARP activity

Analysis

Forensic

Author: Prof Bill Buchanan

Example investigations

seg2 - Ethereal

File Edit View Go Capture Analyze Statistics Help

Filter: tcp.flags.syn == 1 Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
5	0.004633	39.8.29.15	10.0.1.168	TCP	http > 21004 [SYN, ACK] Seq=0 Ack=1 Win=32736 Len=0 MSS=1460
32	0.500413	39.8.29.15	10.0.1.168	TCP	http > 21005 [SYN, ACK] Seq=0 Ack=1 Win=32736 Len=0 MSS=1460
44	0.720199	39.8.29.15	10.0.1.168	TCP	http > 21006 [SYN, ACK] Seq=0 Ack=1 Win=32736 Len=0 MSS=1460
48	0.740278	39.8.29.15	10.0.1.168	TCP	http > 21007 [SYN, ACK] Seq=0 Ack=1 Win=32736 Len=0 MSS=1460
52	0.760518	39.8.29.15	10.0.1.168	TCP	http > 21008 [SYN, ACK] Seq=0 Ack=1 Win=32736 Len=0 MSS=1460
56	0.780501	39.8.29.15	10.0.1.168	TCP	http > 21010 [SYN, ACK] Seq=0 Ack=1 Win=32736 Len=0 MSS=1460
62	0.860525	39.8.29.15	10.0.1.168	TCP	http > 21020 [SYN, ACK] Seq=0 Ack=1 Win=32736 Len=0 MSS=1460
66	0.880305	39.8.29.15	10.0.1.168	TCP	http > 21021 [SYN, ACK] Seq=0 Ack=1 Win=32736 Len=0 MSS=1460
76	1.020540	39.8.29.15	10.0.1.168	TCP	http > 21022 [SYN, ACK] Seq=0 Ack=1 Win=32736 Len=0 MSS=1460
84	1.141232	39.8.29.15	10.0.1.168	TCP	http > 21023 [SYN, ACK] Seq=0 Ack=1 Win=32736 Len=0 MSS=1460
97	1.350033	39.8.29.15	10.0.1.168	TCP	http > 21024 [SYN, ACK] Seq=0 Ack=1 Win=32736 Len=0 MSS=1460
101	1.370022	39.8.29.15	10.0.1.168	TCP	http > 21036 [SYN, ACK] Seq=0 Ack=1 Win=32736 Len=0 MSS=1460
106	1.390747	39.8.29.15	10.0.1.168	TCP	http > 21037 [SYN, ACK] Seq=0 Ack=1 Win=32736 Len=0 MSS=1460
118	1.600456	39.8.29.15	10.0.1.168	TCP	http > 21038 [SYN, ACK] Seq=0 Ack=1 Win=32736 Len=0 MSS=1460
123	1.622301	39.8.29.15	10.0.1.168	TCP	http > 21039 [SYN, ACK] Seq=0 Ack=1 Win=32736 Len=0 MSS=1460
128	1.680198	39.8.29.15	10.0.1.168	TCP	http > 21052 [SYN, ACK] Seq=0 Ack=1 Win=32736 Len=0 MSS=1460
135	1.761588	39.8.29.15	10.0.1.168	TCP	http > 21055 [SYN, ACK] Seq=0 Ack=1 Win=32736 Len=0 MSS=1460
139	1.781256	39.8.29.15	10.0.1.168	TCP	http > 21056 [SYN, ACK] Seq=0 Ack=1 Win=32736 Len=0 MSS=1460

```
⊞ Frame 22645 (60 bytes on wire, 60 bytes captured)
⊞ Ethernet II, Src: 3com_de:54:36 (00:60:97:de:54:36), Dst: 10.0.1.1 (00:0c:ce:85:ab:60)
⊞ Internet Protocol, Src: 39.8.29.15 (39.8.29.15), Dst: 10.0.1.5 (10.0.1.5)
⊞ Transmission Control Protocol, Src Port: http (80), Dst Port: 21556 (21556), Seq: 0, Ack: 1, Len: 0
```

```
0000  00 0c ce 85 ab 60 00 60  97 de 54 36 08 00 45 00   .....`.` ..T6..E.
0010  00 2c 69 36 00 00 40 06  c2 7a 27 08 1d 0f 0a 00   .,i6..@. .z'.....
0020  01 05 00 50 54 34 40 bc  c1 9c 05 1c 58 94 60 12   ...PT4@. ....X.`.
0030  7f e0 14 8d 00 00 02 04  05 b4 05 b4               ........ ....
```

File: "c:\docs\adv_security\notes2005_2006\cour... P: 100000 D: 3498 M: 0

Analysis

Forensic

tcp.flags.syn == 1

Author: Prof Bill Buchanan

seg2 - Ethereal

File Edit View Go Capture Analyze Statistics Help

Filter: tcp.flags.syn == 1 and tcp.flags.ack == 0 Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
1083	15.216535	68.37.75.158	10.0.1.50	TCP	9373 > smtp [SYN] Seq=0 Ack=0 Win=512 Len=0 MSS=1460
1109	15.275240	68.37.75.158	10.0.1.50	TCP	9428 > smtp [SYN] Seq=0 Ack=0 Win=512 Len=0 MSS=1460
1908	24.931707	128.129.31.12	10.0.1.14	TCP	1626 > 22 [SYN] Seq=0 Ack=0 Win=5840 Len=0 MSS=1460 TSV=1306422 TSER=0 WS=2
2378	30.692250	128.129.31.12	10.0.1.16	TCP	3123 > 22 [SYN] Seq=0 Ack=0 Win=5840 Len=0 MSS=1460 TSV=1312183 TSER=0 WS=2
3224	39.308651	67.73.151.50	10.0.1.169	TCP	9429 > smtp [SYN] Seq=0 Ack=0 Win=512 Len=0 MSS=1460
3658	44.148527	66.27.251.21	10.0.1.50	TCP	9430 > smtp [SYN] Seq=0 Ack=0 Win=512 Len=0 MSS=1460
6020	72.981278	66.27.251.21	10.0.1.207	TCP	9553 > finger [SYN] Seq=0 Ack=0 Win=512 Len=0 MSS=1460
8226	99.416849	66.7.248.153	10.0.1.50	TCP	9814 > smtp [SYN] Seq=0 Ack=0 Win=512 Len=0 MSS=1460
10911	130.150324	68.227.33.189	10.0.1.50	TCP	10068 > smtp [SYN] Seq=0 Ack=0 Win=512 Len=0 MSS=1460
10928	130.210549	68.227.33.189	10.0.1.50	TCP	10133 > smtp [SYN] Seq=0 Ack=0 Win=512 Len=0 MSS=1460
10951	130.269541	68.227.33.189	10.0.1.149	TCP	10196 > smtp [SYN] Seq=0 Ack=0 Win=512 Len=0 MSS=1460
13905	162.744772	67.73.151.50	10.0.1.168	TCP	10250 > smtp [SYN] Seq=0 Ack=0 Win=512 Len=0 MSS=1460
14271	167.535930	67.73.151.50	10.0.1.148	TCP	10252 > smtp [SYN] Seq=0 Ack=0 Win=512 Len=0 MSS=1460
14885	176.451177	66.27.251.21	10.0.1.149	TCP	10253 > finger [SYN] Seq=0 Ack=0 Win=512 Len=0 MSS=1460
17658	212.856543	67.115.218.108	10.0.1.84	TCP	10642 > smtp [SYN] Seq=0 Ack=0 Win=512 Len=0 MSS=1460
17671	212.894112	67.115.218.108	10.0.1.169	TCP	10705 > smtp [SYN] Seq=0 Ack=0 Win=512 Len=0 MSS=1460
17684	212.942104	67.115.218.108	10.0.1.207	TCP	10706 > smtp [SYN] Seq=0 Ack=0 Win=512 Len=0 MSS=1460
17695	212.994982	67.115.218.108	10.0.1.194	TCP	10774 > smtp [SYN] Seq=0 Ack=0 Win=512 Len=0 MSS=1460

```
⊞ Frame 2378 (74 bytes on wire, 74 bytes captured)
⊞ Ethernet II, Src: 10.0.1.1 (00:0c:ce:85:ab:60), Dst: 10.0.1.16 (00:01:02:a0:f2:d3)
⊞ Internet Protocol, Src: 128.129.31.12 (128.129.31.12), Dst: 10.0.1.16 (10.0.1.16)
⊞ Transmission Control Protocol, Src Port: 3123 (3123), Dst Port: 22 (22), Seq: 0, Ack: 0, Len: 0

0000  00 01 02 a0 f2 d3 00 0c  ce 85 ab 60 08 00 45 00   ........ ...`..E.
0010  00 3c b2 52 40 00 3f 06  de cc 80 81 1f 0c 0a 00   .<.R@.?. ........
0020  01 10 0c 33 00 16 e7 c6  b7 e5 00 00 00 00 a0 02   ...3.... ........
0030  16 d0 d4 d7 00 00 02 04  05 b4 04 02 08 0a 00 14   ........ ........
0040  05 b7 00 00 00 00 01 03  03 02                     ........ ..
```

File: "c:\docs\adv_security\notes2005_2006\cour... P: 100000 D: 46 M: 0

Forensi

tcp.flags.syn == 1 and tcp.flags.ack == 0

Author: Prof Bill Buchanan

seg1 - Ethereal

File Edit View Go Capture Analyze Statistics Help

Filter: tcp.port == 21 Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
28335	290.636926	44.16.113.50	10.0.1.69	FTP	Request: NLST
28339	290.654026	44.16.113.50	10.0.1.69	TCP	1026 > ftp [ACK] Seq=125 Ack=435 Win=4096 Len=0
28340	290.654443	44.16.113.50	10.0.1.69	TCP	1026 > ftp [ACK] Seq=125 Ack=459 Win=4096 Len=0
28341	290.655277	44.16.113.50	10.0.1.69	FTP	Request: CWD archive
28342	290.655768	44.16.113.50	10.0.1.69	TCP	1026 > ftp [ACK] Seq=138 Ack=488 Win=4096 Len=0
28343	290.655993	44.16.113.50	10.0.1.69	FTP	Request: PORT 172,16,113,50,4,5
28344	290.656401	44.16.113.50	10.0.1.69	FTP	Request: NLST
28349	290.674163	44.16.113.50	10.0.1.69	TCP	1026 > ftp [ACK] Seq=168 Ack=573 Win=4096 Len=0
28350	290.676675	44.16.113.50	10.0.1.69	TCP	1026 > ftp [ACK] Seq=168 Ack=597 Win=4096 Len=0
28351	290.677156	44.16.113.50	10.0.1.69	FTP	Request: CWD music
28352	290.696206	44.16.113.50	10.0.1.69	TCP	1026 > ftp [ACK] Seq=179 Ack=626 Win=4096 Len=0
28353	290.696676	44.16.113.50	10.0.1.69	FTP	Request: PORT 172,16,113,50,4,6

```
⊞ Frame 28335 (60 bytes on wire, 60 bytes captured)
⊟ Ethernet II, Src: Cisco_04:41:bc (00:00:0c:04:41:bc), Dst: 10.0.1.1 (00:0c:ce:85:ab:60)
    Destination: 10.0.1.1 (00:0c:ce:85:ab:60)
    Source: Cisco_04:41:bc (00:00:0c:04:41:bc)
    Type: IP (0x0800)
⊞ Internet Protocol, Src: 44.16.113.50 (44.16.113.50), Dst: 10.0.1.69 (10.0.1.69)
⊟ Transmission Control Protocol, Src Port: 1026 (1026), Dst Port: ftp (21), Seq: 119, Ack: 380, Len: 6
    Source port: 1026 (1026)
    Destination port: ftp (21)
    Sequence number: 119    (relative sequence number)
    [Next sequence number: 125    (relative sequence number)]
    Acknowledgement number: 380    (relative ack number)
    Header length: 20 bytes
  ⊞ Flags: 0x0018 (PSH, ACK)
    Window size: 4096
    Checksum: 0x32c9 [correct]
⊟ File Transfer Protocol (FTP)
  ⊟ NLST\r\n
      Request command: NLST
```

```
0000  00 0c ce 85 ab 60 00 00  0c 04 41 bc 08 00 45 00   .....`.. ..A...E.
0010  00 2e 07 b6 00 00 3b 06  cf 8d 2c 10 71 32 0a 00   ......;. ..,.q2..
0020  01 45 04 02 00 15 2d 57  6c 78 67 a2 10 43 50 18   .E....-W lxg..CP.
0030  10 00 32 c9 00 00 4e 4c  53 54 0d 0a               ..2...NL ST..
```

Forensic

tcp.port. == 21

Author: Prof Bill Buchanan

capture1 - Ethereal

File Edit View Go Capture Analyze Statistics Help

Filter: udp.port == 53 Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
77	17.575797	195.92.195.94	192.168.1.102	DNS	Standard query response A 131.107.113.76
114	31.068585	192.168.1.102	195.92.195.94	DNS	Standard query PTR 103.1.168.192.in-addr.arpa
115	31.109458	195.92.195.94	192.168.1.102	DNS	Standard query response, No such name
131	40.776286	192.168.1.102	195.92.195.94	DNS	Standard query A www.tri.napier.ac.uk
133	40.816157	195.92.195.94	192.168.1.102	DNS	Standard query response CNAME tri.napier.ac.uk A 146.176.1.121
943	67.186499	192.168.1.102	195.92.195.94	DNS	Standard query A www.google.com
944	67.227317	195.92.195.94	192.168.1.102	DNS	Standard query response CNAME www.l.google.com A 66.102.9.104 A 66.102.9.147 A 6
976	129.420758	192.168.1.102	195.92.195.94	DNS	Standard query A ftp2.dcs.napier.ac.uk
977	129.476450	195.92.195.94	192.168.1.102	DNS	Standard query response CNAME titan.napier.ac.uk A 146.176.166.6
978	129.486704	192.168.1.102	195.92.195.94	DNS	Standard query PTR 6.166.176.146.in-addr.arpa
979	129.527025	195.92.195.94	192.168.1.102	DNS	Standard query response PTR www.titan.napier.ac.uk
1027	165.452483	192.168.1.102	195.92.195.94	DNS	Standard query PTR 100.1.168.192.in-addr.arpa
1028	165.493560	195.92.195.94	192.168.1.102	DNS	Standard query response, No such name
1079	223.443918	192.168.1.102	195.92.195.94	DNS	Standard query PTR 94.195.92.195.in-addr.arpa
1080	223.486408	195.92.195.94	192.168.1.102	DNS	Standard query response PTR resolver1.svr.pol.co.uk
1081	223.492797	192.168.1.102	195.92.195.94	DNS	Standard query A www.intel.com
1082	223.520744	195.92.195.94	192.168.1.102	DNS	Standard query response CNAME www.glb.intel.com A 198.175.96.33
1083	233.035639	192.168.1.102	195.92.195.94	DNS	Standard query PTR 94.195.92.195.in-addr.arpa
1084	233.114347	195.92.195.94	192.168.1.102	DNS	Standard query response PTR resolver1.svr.pol.co.uk
1085	233.115488	192.168.1.102	195.92.195.94	DNS	Standard query A www.microsoft.com
1086	233.143326	195.92.195.94	192.168.1.102	DNS	Standard query response CNAME toggle.www.ms.akadns.net CNAME g.www.ms.akadns.net

```
⊞ Frame 1085 (77 bytes on wire, 77 bytes captured)
⊟ Ethernet II, Src: 192.168.1.102 (00:15:00:34:02:f0), Dst: 192.168.1.1 (00:0c:41:f5:23:d5)
    Destination: 192.168.1.1 (00:0c:41:f5:23:d5)
    Source: 192.168.1.102 (00:15:00:34:02:f0)
    Type: IP (0x0800)
⊞ Internet Protocol, Src: 192.168.1.102 (192.168.1.102), Dst: 195.92.195.94 (195.92.195.94)
⊞ User Datagram Protocol, Src Port: 1399 (1399), Dst Port: domain (53)
⊟ Domain Name System (query)
    Transaction ID: 0x0002
  ⊞ Flags: 0x0100 (Standard query)
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
```

```
0000  00 0c 41 f5 23 d5 00 15  00 34 02 f0 08 00 45 00   ..A.#... .4....E.
0010  00 3f 0a 87 00 00 80 11  e7 5d c0 a8 01 66 c3 5c   .?...... .]...f.\
0020  c3 5e 05 77 00 35 00 2b  01 3d 00 02 01 00 00 01   .^.w.5.+ .=......
0030  00 00 00 00 00 00 03 77  77 77 09 6d 69 63 72 6f   .......w ww.micro
0040  73 6f 66 74 03 63 6f 6d  00 00 01 00 01            soft.com .....
```

DNS Query

Forens

Udp.port == 53

Author: Prof Bill Buchanan

capture1 - Ethereal

File Edit View Go Capture Analyze Statistics Help

Filter: udp.port == 53 Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
77	17.575797	195.92.195.94	192.168.1.102	DNS	Standard query response A 131.107.113.76
114	31.068585	192.168.1.102	195.92.195.94	DNS	Standard query PTR 103.1.168.192.in-addr.arpa
115	31.109458	195.92.195.94	192.168.1.102	DNS	Standard query response, No such name
131	40.776286	192.168.1.102	195.92.195.94	DNS	Standard query A www.tri.napier.ac.uk
133	40.816157	195.92.195.94	192.168.1.102	DNS	Standard query response CNAME tri.napier.ac.uk A 146.176.1.121
943	67.186499	192.168.1.102	195.92.195.94	DNS	Standard query A www.google.com
944	67.227317	195.92.195.94	192.168.1.102	DNS	Standard query response CNAME www.l.google.com A 66.102.9.104 A 66.102.9.147 A 6
976	129.420758	192.168.1.102	195.92.195.94	DNS	Standard query A ftp2.dcs.napier.ac.uk
977	129.476450	195.92.195.94	192.168.1.102	DNS	Standard query response CNAME titan.napier.ac.uk A 146.176.166.6
978	129.486704	192.168.1.102	195.92.195.94	DNS	Standard query PTR 6.166.176.146.in-addr.arpa
979	129.527025	195.92.195.94	192.168.1.102	DNS	Standard query response PTR www.titan.napier.ac.uk
1027	165.452483	192.168.1.102	195.92.195.94	DNS	Standard query PTR 100.1.168.192.in-addr.arpa
1028	165.493560	195.92.195.94	192.168.1.102	DNS	Standard query response, No such name
1079	223.443918	192.168.1.102	195.92.195.94	DNS	Standard query PTR 94.195.92.195.in-addr.arpa
1080	223.486408	195.92.195.94	192.168.1.102	DNS	Standard query response PTR resolver1.svr.pol.co.uk
1081	223.492797	192.168.1.102	195.92.195.94	DNS	Standard query A www.intel.com
1082	223.520744	195.92.195.94	192.168.1.102	DNS	Standard query response CNAME www.glb.intel.com A 198.175.96.33
1083	233.035639	192.168.1.102	195.92.195.94	DNS	Standard query PTR 94.195.92.195.in-addr.arpa
1084	233.114347	195.92.195.94	192.168.1.102	DNS	Standard query response PTR resolver1.svr.pol.co.uk
1085	233.115488	192.168.1.102	195.92.195.94	DNS	Standard query A www.microsoft.com
1086	233.143326	195.92.195.94	192.168.1.102	DNS	Standard query response CNAME toggle.www.ms.akadns.net CNAME g.www.ms.akadns.net

```
⊞ Frame 1086 (552 bytes on wire, 552 bytes captured)
⊟ Ethernet II, Src: 192.168.1.1 (00:0c:41:f5:23:d5), Dst: 192.168.1.102 (00:15:00:34:02:f0)
    Destination: 192.168.1.102 (00:15:00:34:02:f0)
    Source: 192.168.1.1 (00:0c:41:f5:23:d5)
    Type: IP (0x0800)
⊞ Internet Protocol, Src: 195.92.195.94 (195.92.195.94), Dst: 192.168.1.102 (192.168.1.102)
⊞ User Datagram Protocol, Src Port: domain (53), Dst Port: 1399 (1399)
⊟ Domain Name System (response)
    Transaction ID: 0x0002
  ⊞ Flags: 0x8180 (Standard query response, No error)
    Questions: 1
    Answer RRs: 11
    Authority RRs: 11
```

```
0000  00 15 00 34 02 f0 00 0c  41 f5 23 d5 08 00 45 00   ...4.... A.#...E.
0010  02 1a 00 00 40 00 3e 11  f2 09 c3 5c c3 5e c0 a8   ....@.>. ...\.^..
0020  01 66 00 35 05 77 02 06  ff 52 00 02 81 80 00 01   .f.5.w.. .R......
0030  00 0b 00 0b 00 04 03 77  77 77 09 6d 69 63 72 6f   .......w ww.micro
0040  73 6f 66 74 03 63 6f 6d  00 00 01 00 01 c0 0c 00   soft.com ........
```

DNS Response

Forensi

Udp.port == 53

Author: Prof Bill Buchanan

capture1 - Ethereal

File Edit View Go Capture Analyze Statistics Help

Filter: udp.port == 53 Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
77	17.575797	195.92.195.94	192.168.1.102	DNS	Standard query response A 131.107.113.76
114	31.068585	192.168.1.102	195.92.195.94	DNS	Standard query PTR 103.1.168.192.in-addr.arpa
115	31.109458	195.92.195.94	192.168.1.102	DNS	Standard query response, No such name
131	40.776286	192.168.1.102	195.92.195.94	DNS	Standard query A www.tri.napier.ac.uk
133	40.816157	195.92.195.94	192.168.1.102	DNS	Standard query response CNAME tri.napier.ac.uk A 146.176.1.121
943	67.186499	192.168.1.102	195.92.195.94	DNS	Standard query A www.google.com
944	67.227317	195.92.195.94	192.168.1.102	DNS	Standard query response CNAME www.l.google.com A 66.102.9.104 A 66.102.9.147 A 6
976	129.420758	192.168.1.102	195.92.195.94	DNS	Standard query A ftp2.dcs.napier.ac.uk
977	129.476450	195.92.195.94	192.168.1.102	DNS	Standard query response CNAME titan.napier.ac.uk A 146.176.166.6
978	129.486704	192.168.1.102	195.92.195.94	DNS	Standard query PTR 6.166.176.146.in-addr.arpa
979	129.527025	195.92.195.94	192.168.1.102	DNS	Standard query response PTR www.titan.napier.ac.uk
1027	165.452483	192.168.1.102	195.92.195.94	DNS	Standard query PTR 100.1.168.192.in-addr.arpa
1028	165.493560	195.92.195.94	192.168.1.102	DNS	Standard query response, No such name
1079	223.443918	192.168.1.102	195.92.195.94	DNS	Standard query PTR 94.195.92.195.in-addr.arpa
1080	223.486408	195.92.195.94	192.168.1.102	DNS	Standard query response PTR resolver1.svr.pol.co.uk
1081	223.492797	192.168.1.102	195.92.195.94	DNS	Standard query A www.intel.com
1082	223.520744	195.92.195.94	192.168.1.102	DNS	Standard query response CNAME www.glb.intel.com A 198.175.96.33
1083	233.035639	192.168.1.102	195.92.195.94	DNS	Standard query PTR 94.195.92.195.in-addr.arpa
1084	233.114347	195.92.195.94	192.168.1.102	DNS	Standard query response PTR resolver1.svr.pol.co.uk
1085	233.115488	192.168.1.102	195.92.195.94	DNS	Standard query A www.microsoft.com
1086	233.143326	195.92.195.94	192.168.1.102	DNS	Standard query response CNAME toggle.www.ms.akadns.net CNAME g.www.ms.akadns.net

```
Additional RRs: 4
⊞ Queries
⊟ Answers
  ⊞ www.microsoft.com: type CNAME, class IN, cname toggle.www.ms.akadns.net
  ⊞ toggle.www.ms.akadns.net: type CNAME, class IN, cname g.www.ms.akadns.net
  ⊞ g.www.ms.akadns.net: type CNAME, class IN, cname lb1.www.ms.akadns.net
  ⊞ lb1.www.ms.akadns.net: type A, class IN, addr 207.46.18.30
  ⊞ lb1.www.ms.akadns.net: type A, class IN, addr 207.46.225.60
  ⊞ lb1.www.ms.akadns.net: type A, class IN, addr 207.46.19.30
  ⊞ lb1.www.ms.akadns.net: type A, class IN, addr 207.46.20.60
  ⊞ lb1.www.ms.akadns.net: type A, class IN, addr 207.46.19.60
  ⊞ lb1.www.ms.akadns.net: type A, class IN, addr 207.46.199.30
  ⊞ lb1.www.ms.akadns.net: type A, class IN, addr 207.46.198.30
```

```
0040  73 6f 66 74 03 63 6f 6d  00 00 01 00 01 c0 0c 00   soft.com .....
0050  05 00 01 00 00 0b 0e 00  1a 06 74 6f 67 67 6c 65   ........ ..toggle
0060  03 77 77 77 02 6d 73 06  61 6b 61 64 6e 73 03 6e   .www.ms. akadns.n
0070  65 74 00 c0 2f 00 05 00  01 00 00 00 ec 00 04 01   et../... ........
0080  67 c0 36 c0 55 00 05 00  01 00 00 00 ec 00 06 03   g.6.U... ........
```

IP addresses returned

Forensic

Udp.port == 53

Author: Prof Bill Buchanan

seg2 - Ethereal

File Edit View Go Capture Analyze Statistics Help

Filter: ip.addr == 68.37.75.158 Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
1083	15.216535	68.37.75.158	10.0.1.50	TCP	9373 > smtp [SYN] Seq=0 Ack=0 Win=512 Len=0 MSS=1460
1085	15.217603	68.37.75.158	10.0.1.50	TCP	9373 > smtp [ACK] Seq=1 Ack=0 Win=32120 Len=0
1089	15.233285	68.37.75.158	10.0.1.50	SMTP	Command: EHLO jupiter.cherry.org
1091	15.233900	68.37.75.158	10.0.1.50	SMTP	Command: HELO jupiter.cherry.org
1093	15.234651	68.37.75.158	10.0.1.50	SMTP	Command: MAIL From:<henningt@jupiter.cherry.org>
1095	15.252584	68.37.75.158	10.0.1.50	SMTP	Command: RCPT To:<yvonnej@zeno.eyrie.af.mil>
1097	15.253648	68.37.75.158	10.0.1.50	SMTP	Command: DATA
1099	15.254919	68.37.75.158	10.0.1.50	SMTP	Message Body
1101	15.271975	68.37.75.158	10.0.1.50	SMTP	Message Body
1103	15.273001	68.37.75.158	10.0.1.50	SMTP	Message Body
1105	15.273987	68.37.75.158	10.0.1.50	TCP	9373 > smtp [FIN, ACK] Seq=927 Ack=380 Win=32696 Len=0
1108	15.274909	68.37.75.158	10.0.1.50	TCP	9373 > smtp [ACK] Seq=928 Ack=381 Win=32695 Len=0
1109	15.275240	68.37.75.158	10.0.1.50	TCP	9428 > smtp [SYN] Seq=0 Ack=0 Win=512 Len=0 MSS=1460
1110	15.275894	68.37.75.158	10.0.1.50	TCP	9428 > smtp [ACK] Seq=1 Ack=0 Win=32120 Len=0
1111	15.276573	68.37.75.158	10.0.1.50	SMTP	Command: EHLO jupiter.cherry.org
1112	15.277968	68.37.75.158	10.0.1.50	SMTP	Command: MAIL From:<henningt@jupiter.cherry.org>
1113	15.278975	68.37.75.158	10.0.1.50	SMTP	Command: RCPT To:<lupitam@pascal.eyrie.af.mil>
1114	15.292232	68.37.75.158	10.0.1.50	SMTP	Command: DATA

```
⊞ Frame 2583 (60 bytes on wire, 60 bytes captured)
⊞ Ethernet II, Src: DellComp_a3:58:23 (00:c0:4f:a3:58:23), Dst: 10.0.1.1 (00:0c:ce:85:ab:60)
⊞ Internet Protocol, Src: 68.37.75.158 (68.37.75.158), Dst: 10.0.1.207 (10.0.1.207)
⊟ Transmission Control Protocol, Src Port: smtp (25), Dst Port: 24230 (24230), Seq: 0, Ack: 1, Len: 0
    Source port: smtp (25)
    Destination port: 24230 (24230)
    Sequence number: 0    (relative sequence number)
    Acknowledgement number: 1    (relative ack number)
    Header length: 24 bytes
  ⊞ Flags: 0x0012 (SYN, ACK)
    Window size: 32736
    Checksum: 0x9fd2 [correct]
  ⊞ Options: (4 bytes)
```

```
0000  00 0c ce 85 ab 60 00 c0  4f a3 58 23 08 00 45 00   .....`.. O.X#..E.
0010  00 2c f1 73 00 00 40 06  ed c6 44 25 4b 9e 0a 00   .,.s..@. ..D%K...
0020  01 cf 00 19 5e a6 f2 78  16 2d 98 c7 dc a4 60 12   ....^..x .-....`.
0030  7f e0 9f d2 00 00 02 04  05 b4 05 b4               ........ ....
```

Internet Protocol (ip), 20 bytes | P: 100000 D: 113 M: 0

Foren

ip.addr == 68.37.75.158

Author: Prof Bill Buchanan

IP filter

seg2 - Ethereal

File Edit View Go Capture Analyze Statistics Help

Filter: ip.addr == 68.37.75.158 and ip.addr ==10.0.1.207 Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
2583	32.866014	68.37.75.158	10.0.1.207	TCP	smtp > 24230 [SYN, ACK] Seq=0 Ack=1 Win=32736 Len=0 MSS=1460
2584	32.884567	68.37.75.158	10.0.1.207	SMTP	Response: 220 jupiter.cherry.org Sendmail 4.1/SMI-4.1 ready at Mon, 1 Jun 1998 11:40:14 -0400
2585	32.884923	68.37.75.158	10.0.1.207	SMTP	Response: 500 Command unrecognized
2586	32.885171	68.37.75.158	10.0.1.207	SMTP	Response: 250 (pigeon.eyrie.af.mil) pleased to meet you.
2587	32.885390	68.37.75.158	10.0.1.207	SMTP	Response: 250 <juttar@pigeon.eyrie.af.mil>... Sender Ok
2588	32.885607	68.37.75.158	10.0.1.207	SMTP	Response: 250 <edwinav@jupiter.cherry.org> OK
2589	32.885818	68.37.75.158	10.0.1.207	TCP	smtp > 24230 [ACK] Seq=244 Ack=137 Win=32736 Len=0
2590	32.885921	68.37.75.158	10.0.1.207	SMTP	Response: 354 Enter mail, end with "." on a line by itself
2591	32.914918	68.37.75.158	10.0.1.207	TCP	smtp > 24230 [ACK] Seq=294 Ack=1161 Win=32736 Len=0
2592	32.915576	68.37.75.158	10.0.1.207	SMTP	Response: 250 Mail accepted
2593	32.916206	68.37.75.158	10.0.1.207	SMTP	Response: 221 Closing connection
2594	32.916510	68.37.75.158	10.0.1.207	TCP	smtp > 24230 [FIN, ACK] Seq=337 Ack=1727 Win=32736 Len=0
2595	32.918331	68.37.75.158	10.0.1.207	TCP	smtp > 24230 [ACK] Seq=338 Ack=1728 Win=32735 Len=0

```
⊞ Frame 2583 (60 bytes on wire, 60 bytes captured)
⊞ Ethernet II, Src: DellComp_a3:58:23 (00:c0:4f:a3:58:23), Dst: 10.0.1.1 (00:0c:ce:85:ab:60)
⊞ Internet Protocol, Src: 68.37.75.158 (68.37.75.158), Dst: 10.0.1.207 (10.0.1.207)
⊟ Transmission Control Protocol, Src Port: smtp (25), Dst Port: 24230 (24230), Seq: 0, Ack: 1, Len: 0
    Source port: smtp (25)
    Destination port: 24230 (24230)
    Sequence number: 0    (relative sequence number)
    Acknowledgement number: 1    (relative ack number)
    Header length: 24 bytes
  ⊞ Flags: 0x0012 (SYN, ACK)
    Window size: 32736
    Checksum: 0x9fd2 [correct]
  ⊞ Options: (4 bytes)
```

```
0000  00 0c ce 85 ab 60 00 c0  4f a3 58 23 08 00 45 00   .....`.. O.X#..E.
0010  00 2c f1 73 00 00 40 06  ed c6 44 25 4b 9e 0a 00   .,.s..@. ..D%K...
0020  01 cf 00 19 5e a6 f2 78  16 2d 98 c7 dc a4 60 12   ....^..x .-....`.
0030  7f e0 9f d2 00 00 02 04  05 b4 05 b4               ........ ....
```

File: "c:\docs\adv_security\notes2005_2006\cour... P: 100000 D: 13 M: 0

ip.addr == 68.37.75.158 and ip.addr ==10.0.1.207

Author: Prof Bill Buchanan

IP filter

seg2 - Ethereal

File Edit View Go Capture Analyze Statistics Help

Filter: eth.src == 00:60:97:de:54:36 Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
1	0.000000	9.9.20.248	10.0.1.168	TCP	[TCP segment of a reassembled PDU]
2	0.000187	9.9.20.248	10.0.1.168	HTTP	HTTP/1.1 200 OK (GIF89a)
3	0.000878	9.9.20.248	10.0.1.168	TCP	http > 21003 [FIN, ACK] Seq=1304 Ack=0 Win=32736 Len=0
4	0.001879	9.9.20.248	10.0.1.168	TCP	http > 21003 [ACK] Seq=1305 Ack=1 Win=32735 Len=0
5	0.004633	39.8.29.15	10.0.1.168	TCP	http > 21004 [SYN, ACK] Seq=0 Ack=1 Win=32736 Len=0 MSS=1460
6	0.005719	39.8.29.15	10.0.1.168	TCP	http > 21004 [ACK] Seq=1 Ack=163 Win=32736 Len=0
7	0.030106	39.8.29.15	10.0.1.168	HTTP	HTTP/1.0 200 OK (text/html)
8	0.060060	39.8.29.15	10.0.1.168	HTTP	Continuation or non-HTTP traffic
9	0.090070	39.8.29.15	10.0.1.168	HTTP	Continuation or non-HTTP traffic
10	0.110081	39.8.29.15	10.0.1.168	HTTP	Continuation or non-HTTP traffic
11	0.130116	39.8.29.15	10.0.1.168	HTTP	Continuation or non-HTTP traffic
12	0.160099	39.8.29.15	10.0.1.168	HTTP	Continuation or non-HTTP traffic
13	0.180085	39.8.29.15	10.0.1.168	HTTP	Continuation or non-HTTP traffic
14	0.200145	39.8.29.15	10.0.1.168	HTTP	Continuation or non-HTTP traffic
15	0.230150	39.8.29.15	10.0.1.168	HTTP	Continuation or non-HTTP traffic
16	0.250083	39.8.29.15	10.0.1.168	HTTP	Continuation or non-HTTP traffic
17	0.270093	39.8.29.15	10.0.1.168	HTTP	Continuation or non-HTTP traffic
18	0.300171	39.8.29.15	10.0.1.168	HTTP	Continuation or non-HTTP traffic

```
⊞ Frame 1 (1078 bytes on wire, 1078 bytes captured)
⊟ Ethernet II, Src: 3com_de:54:36 (00:60:97:de:54:36), Dst: 10.0.1.1 (00:0c:ce:85:ab:60)
    Destination: 10.0.1.1 (00:0c:ce:85:ab:60)
    Source: 3com_de:54:36 (00:60:97:de:54:36)
    Type: IP (0x0800)
⊞ Internet Protocol, Src: 9.9.20.248 (9.9.20.248), Dst: 10.0.1.168 (10.0.1.168)
⊟ Transmission Control Protocol, Src Port: http (80), Dst Port: 21003 (21003), Seq: 0, Ack: 0, Len: 1024
    Source port: http (80)
    Destination port: 21003 (21003)
    Sequence number: 0    (relative sequence number)
    [Next sequence number: 1024    (relative sequence number)]
    Acknowledgement number: 0    (relative ack number)
    Header length: 20 bytes
  ⊞ Flags: 0x0018 (PSH, ACK)
    Window size: 32736
    Checksum: 0x75f5 [correct]
    [Reassembled PDU in frame: 2]
```

```
0000  00 0c ce 85 ab 60 00 60  97 de 54 36 08 00 45 00   .....`.` ..T6..E.
0010  04 28 15 d2 40 00 40 06  f7 55 09 09 14 f8 0a 00   .(..@.@. .U......
0020  01 a8 00 50 52 0b aa 2c  76 84 a9 88 48 97 50 18   ...PR.., v...H.P.
0030  7f e0 75 f5 00 00 48 54  54 50 2f 31 2e 31 20 32   ..u...HT TP/1.1 2
0040  30 30 20 4f 4b 0d 0a 53  65 72 76 65 72 3a 20 4d   00 OK..S erver: M
0050  69 63 72 6f 73 6f 66 74  2d 49 49 53 2f 34 2e 30   icrosoft -IIS/4.0
0060  0d 0a 44 61 74 65 3a 20  4d 6f 6e 20 4a 75 6e 20   ..Date:  Mon Jun
0070  20 31 20 31 31 3a 33 36  3a 34 31 20 45 44 54 20    1 11:36 :41 EDT
0080  31 39 39 38 0a 43 6f 6e  74 65 6e 74 2d 54 79 70   1998.Con tent-Typ
0090  65 3a 20 69 6d 61 67 65  2f 67 69 66 0d 0a 41 63   e: image /gif..Ac
00a0  63 65 70 74 2d 52 61 6e  67 65 73 3a 20 62 79 74   cept-Ran ges: byt
00b0  65 73 0d 0a 4c 61 73 74  2d 4d 6f 64 69 66 69 65   es..Last -Modifie
00c0  64 3a 20 54 68 75 2c 20  31 39 20 4d 61 72 20 31   d: Thu,  19 Mar 1
00d0  39 39 38 20 32 30 3a 30  35 3a 32 30 20 47 4d 54   998 20:0 5:20 GMT
```

File: "c:\docs\adv_security\notes2005_2006\cour... P: 100000 D: 9317 M: 0

Forensic Analysis

eth.src == 00:60:97:de:54:36

Author: Prof Bill Buchanan

Ethernet filter

seg2 - Ethereal

File Edit View Go Capture Analyze Statistics Help

Filter: eth.src == 00:0c:ce:85:ab:60 Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
19	0.316834	128.129.31.12	10.0.1.33	TCP	2730 > 22 [ACK] Seq=0 Ack=0 Win=9956 Len=0 TSV=1281805 TSER=23999752
27	0.466620	10.0.1.1	10.0.1.1	LOOP	Reply
141	1.823842	10.0.1.1	Broadcast	ARP	Who has 10.0.1.168? Tell 10.0.1.1
188	2.327515	128.129.31.12	10.0.1.33	TCP	2730 > 22 [ACK] Seq=0 Ack=256 Win=9956 Len=0 TSV=1283816 TSER=23999953
303	3.689337	10.0.1.1	Broadcast	ARP	Who has 10.0.1.234? Tell 10.0.1.1
338	4.337518	128.129.31.12	10.0.1.33	TCP	2730 > 22 [ACK] Seq=0 Ack=528 Win=9956 Len=0 TSV=1285826 TSER=24000154
469	5.693261	10.0.1.1	Broadcast	ARP	Who has 10.0.1.234? Tell 10.0.1.1
483	5.762739	10.0.1.1	Broadcast	ARP	Who has 10.0.1.204? Tell 10.0.1.1
539	6.348391	128.129.31.12	10.0.1.33	TCP	2730 > 22 [ACK] Seq=0 Ack=832 Win=9956 Len=0 TSV=1287837 TSER=24000355
559	6.562507	10.0.1.1	Broadcast	ARP	Who has 10.0.1.148? Tell 10.0.1.1
576	6.807662	10.0.1.1	224.0.0.5	OSPF	Hello Packet
649	7.702327	10.0.1.1	Broadcast	ARP	Who has 10.0.1.234? Tell 10.0.1.1
695	8.358031	128.129.31.12	10.0.1.33	TCP	2730 > 22 [ACK] Seq=0 Ack=1056 Win=9956 Len=0 TSV=1289847 TSER=24000556
716	8.587684	10.0.1.1	Broadcast	ARP	Who has 10.0.1.148? Tell 10.0.1.1
809	9.673486	10.0.1.1	Broadcast	ARP	Who has 10.0.1.204? Tell 10.0.1.1
852	10.370067	128.129.31.12	10.0.1.33	TCP	2730 > 22 [ACK] Seq=0 Ack=1360 Win=9956 Len=0 TSV=1291859 TSER=24000757
861	10.532142	10.0.1.1	10.0.1.1	LOOP	Reply
892	10.964032	10.0.1.1	Broadcast	ARP	Who has 10.0.1.168? Tell 10.0.1.1

```
⊞ Frame 19 (66 bytes on wire, 66 bytes captured)
⊟ Ethernet II, Src: 10.0.1.1 (00:0c:ce:85:ab:60), Dst: 10.0.1.33 (00:50:04:35:59:1d)
    Destination: 10.0.1.33 (00:50:04:35:59:1d)
    Source: 10.0.1.1 (00:0c:ce:85:ab:60)
    Type: IP (0x0800)
⊞ Internet Protocol, Src: 128.129.31.12 (128.129.31.12), Dst: 10.0.1.33 (10.0.1.33)
⊟ Transmission Control Protocol, Src Port: 2730 (2730), Dst Port: 22 (22), Seq: 0, Ack: 0, Len: 0
    Source port: 2730 (2730)
    Destination port: 22 (22)
    Sequence number: 0    (relative sequence number)
    Acknowledgement number: 0    (relative ack number)
    Header length: 32 bytes
  ⊞ Flags: 0x0010 (ACK)
    Window size: 9956
    Checksum: 0x74a3 [correct]
  ⊞ Options: (12 bytes)
```

```
0000  00 50 04 35 59 1d 00 0c  ce 85 ab 60 08 00 45 10   .P.5Y... ...`..E.
0010  00 34 4d bd 40 00 3f 06  43 49 80 81 1f 0c 0a 00   .4M.@.?. CI......
0020  01 21 0a aa 00 16 d0 6e  69 ea 0f 76 16 62 80 10   .!.....n i..v.b..
0030  26 e4 74 a3 00 00 01 01  08 0a 00 13 8f 0d 01 6e   &.t..... .......n
0040  35 08                                              5.
```

File: "c:\docs\adv_security\notes2005_2006\cour... P: 100000 D: 345 M: 0

Forensic

eth.src == 00:0c:ce:85:ab:60

Author: Prof Bill Buchanan

Ethernet filter

seg2 - Ethereal

File Edit View Go Capture Analyze Statistics Help

Filter: eth.dst == ff:ff:ff:ff:ff:ff Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
141	1.823842	10.0.1.1	Broadcast	ARP	Who has 10.0.1.168? Tell 10.0.1.1
303	3.689337	10.0.1.1	Broadcast	ARP	Who has 10.0.1.234? Tell 10.0.1.1
469	5.693261	10.0.1.1	Broadcast	ARP	Who has 10.0.1.234? Tell 10.0.1.1
483	5.762739	10.0.1.1	Broadcast	ARP	Who has 10.0.1.204? Tell 10.0.1.1
559	6.562507	10.0.1.1	Broadcast	ARP	Who has 10.0.1.148? Tell 10.0.1.1
649	7.702327	10.0.1.1	Broadcast	ARP	Who has 10.0.1.234? Tell 10.0.1.1
716	8.587684	10.0.1.1	Broadcast	ARP	Who has 10.0.1.148? Tell 10.0.1.1
809	9.673486	10.0.1.1	Broadcast	ARP	Who has 10.0.1.204? Tell 10.0.1.1
892	10.964032	10.0.1.1	Broadcast	ARP	Who has 10.0.1.168? Tell 10.0.1.1
980	12.968362	10.0.1.1	Broadcast	ARP	Who has 10.0.1.168? Tell 10.0.1.1
1069	14.983393	10.0.1.1	Broadcast	ARP	Who has 10.0.1.168? Tell 10.0.1.1
1086	15.221225	10.0.1.1	Broadcast	ARP	Who has 10.0.1.50? Tell 10.0.1.1
1087	15.221837	10.0.1.1	Broadcast	ARP	Who has 10.0.1.158? Tell 10.0.1.1
1122	15.321193	10.0.1.1	Broadcast	ARP	Who has 10.0.1.204? Tell 10.0.1.1
1134	15.404541	10.0.1.1	Broadcast	ARP	Who has 10.0.1.87? Tell 10.0.1.1
1221	16.184625	10.0.1.1	Broadcast	ARP	Who has 10.0.1.169? Tell 10.0.1.1
1231	16.243661	10.0.1.1	Broadcast	ARP	Who has 10.0.1.234? Tell 10.0.1.1
1386	18.044130	10.0.1.1	Broadcast	ARP	Who has 10.0.1.168? Tell 10.0.1.1
1471	18.684471	10.0.1.1	Broadcast	ARP	Who has 10.0.1.169? Tell 10.0.1.1
1478	18.721807	10.0.1.1	Broadcast	ARP	Who has 10.0.1.132? Tell 10.0.1.1
1495	19.042875	10.0.1.1	Broadcast	ARP	Who has 10.0.1.204? Tell 10.0.1.1

```
⊞ Frame 141 (60 bytes on wire, 60 bytes captured)
⊟ Ethernet II, Src: 10.0.1.1 (00:0c:ce:85:ab:60), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
    Destination: Broadcast (ff:ff:ff:ff:ff:ff)
    Source: 10.0.1.1 (00:0c:ce:85:ab:60)
    Type: ARP (0x0806)
    Trailer: 000000000000000000000000000000000000
⊟ Address Resolution Protocol (request)
    Hardware type: Ethernet (0x0001)
    Protocol type: IP (0x0800)
    Hardware size: 6
    Protocol size: 4
```

```
0000  ff ff ff ff ff ff 00 0c  ce 85 ab 60 08 06 00 01   ........ ... ....
0010  08 00 06 04 00 01 00 0c  ce 85 ab 60 0a 00 01 01   ........ ... ....
0020  00 00 00 00 00 00 0a 00  01 a8 00 00 00 00 00 00   ........ ........
0030  00 00 00 00 00 00 00 00  00 00 00 00               ........ ....
```

Forensic

eth.dst == ff:ff:ff:ff:ff:ff

Author: Prof Bill Buchanan

Ethernet filter

seg2 - Ethereal

File Edit View Go Capture Analyze Statistics Help

Filter: arp.opcode Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
141	1.823842	10.0.1.1	Broadcast	ARP	Who has 10.0.1.168? Tell 10.0.1.1
303	3.689337	10.0.1.1	Broadcast	ARP	Who has 10.0.1.234? Tell 10.0.1.1
469	5.693261	10.0.1.1	Broadcast	ARP	Who has 10.0.1.234? Tell 10.0.1.1
483	5.762739	10.0.1.1	Broadcast	ARP	Who has 10.0.1.204? Tell 10.0.1.1
559	6.562507	10.0.1.1	Broadcast	ARP	Who has 10.0.1.148? Tell 10.0.1.1
649	7.702327	10.0.1.1	Broadcast	ARP	Who has 10.0.1.234? Tell 10.0.1.1
716	8.587684	10.0.1.1	Broadcast	ARP	Who has 10.0.1.148? Tell 10.0.1.1
809	9.673486	10.0.1.1	Broadcast	ARP	Who has 10.0.1.204? Tell 10.0.1.1
892	10.964032	10.0.1.1	Broadcast	ARP	Who has 10.0.1.168? Tell 10.0.1.1
980	12.968362	10.0.1.1	Broadcast	ARP	Who has 10.0.1.168? Tell 10.0.1.1
1069	14.983393	10.0.1.1	Broadcast	ARP	Who has 10.0.1.168? Tell 10.0.1.1
1086	15.221225	10.0.1.1	Broadcast	ARP	Who has 10.0.1.50? Tell 10.0.1.1
1087	15.221837	10.0.1.1	Broadcast	ARP	Who has 10.0.1.158? Tell 10.0.1.1
1122	15.321193	10.0.1.1	Broadcast	ARP	Who has 10.0.1.204? Tell 10.0.1.1
1134	15.404541	10.0.1.1	Broadcast	ARP	Who has 10.0.1.87? Tell 10.0.1.1
1221	16.184625	10.0.1.1	Broadcast	ARP	Who has 10.0.1.169? Tell 10.0.1.1
1231	16.243661	10.0.1.1	Broadcast	ARP	Who has 10.0.1.234? Tell 10.0.1.1
1386	18.044130	10.0.1.1	Broadcast	ARP	Who has 10.0.1.168? Tell 10.0.1.1

```
⊞ Frame 141 (60 bytes on wire, 60 bytes captured)
⊟ Ethernet II, Src: 10.0.1.1 (00:0c:ce:85:ab:60), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
    Destination: Broadcast (ff:ff:ff:ff:ff:ff)
    Source: 10.0.1.1 (00:0c:ce:85:ab:60)
    Type: ARP (0x0806)
    Trailer: 000000000000000000000000000000000000
⊞ Address Resolution Protocol (request)
```

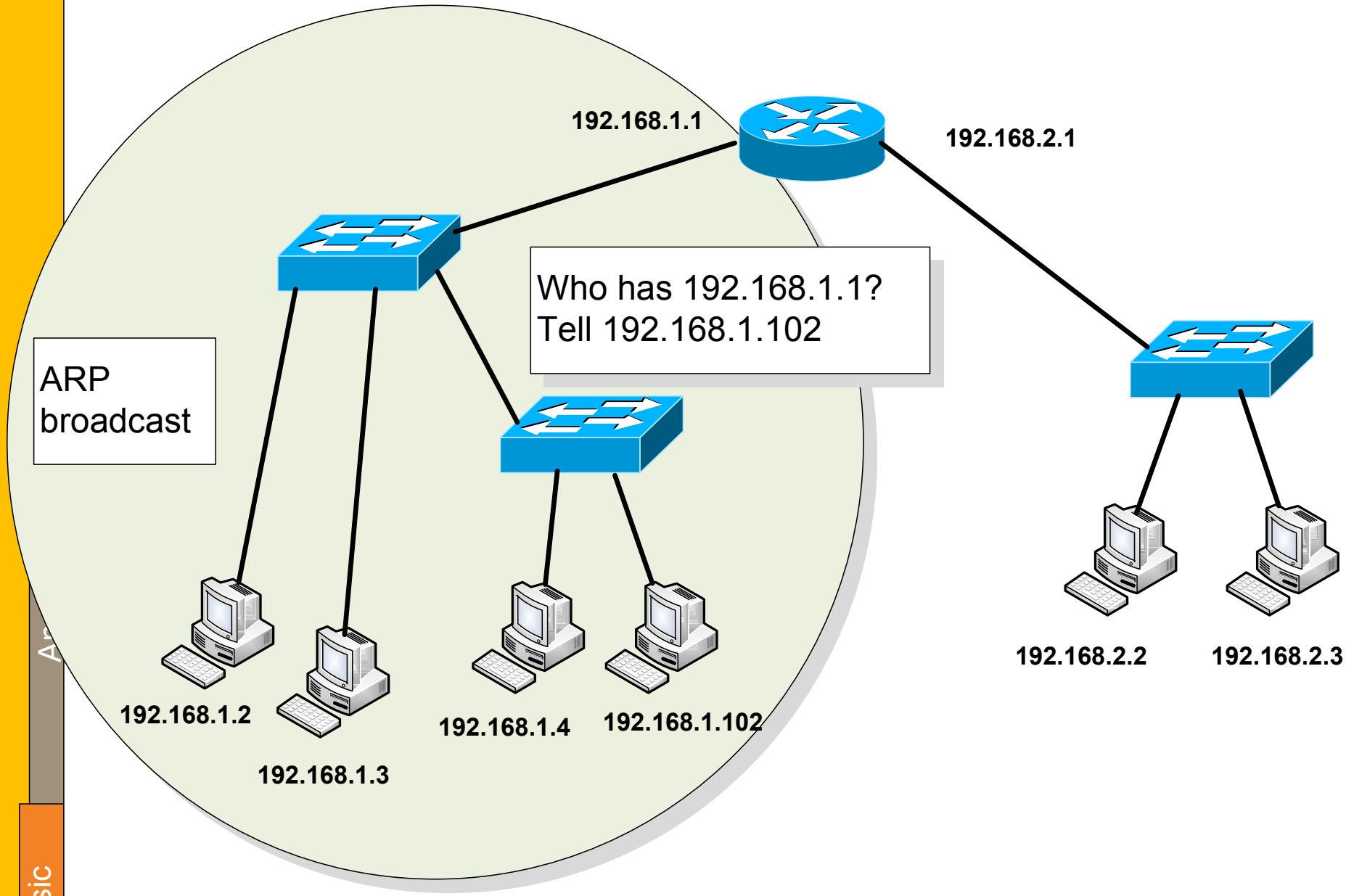
```
0000  ff ff ff ff ff ff 00 0c  ce 85 ab 60 08 06 00 01   ........ ...`....
0010  08 00 06 04 00 01 00 0c  ce 85 ab 60 0a 00 01 01   ........ ...`....
0020  00 00 00 00 00 00 00 0a  01 a8 00 00 00 00 00 00   ........ ........
0030  00 00 00 00 00 00 00 00  00 00 00 00               ........ ....
```

File: "c:\docs\adv_security\notes2005_2006\cour... P: 100000 D: 147 M: 0

Foren

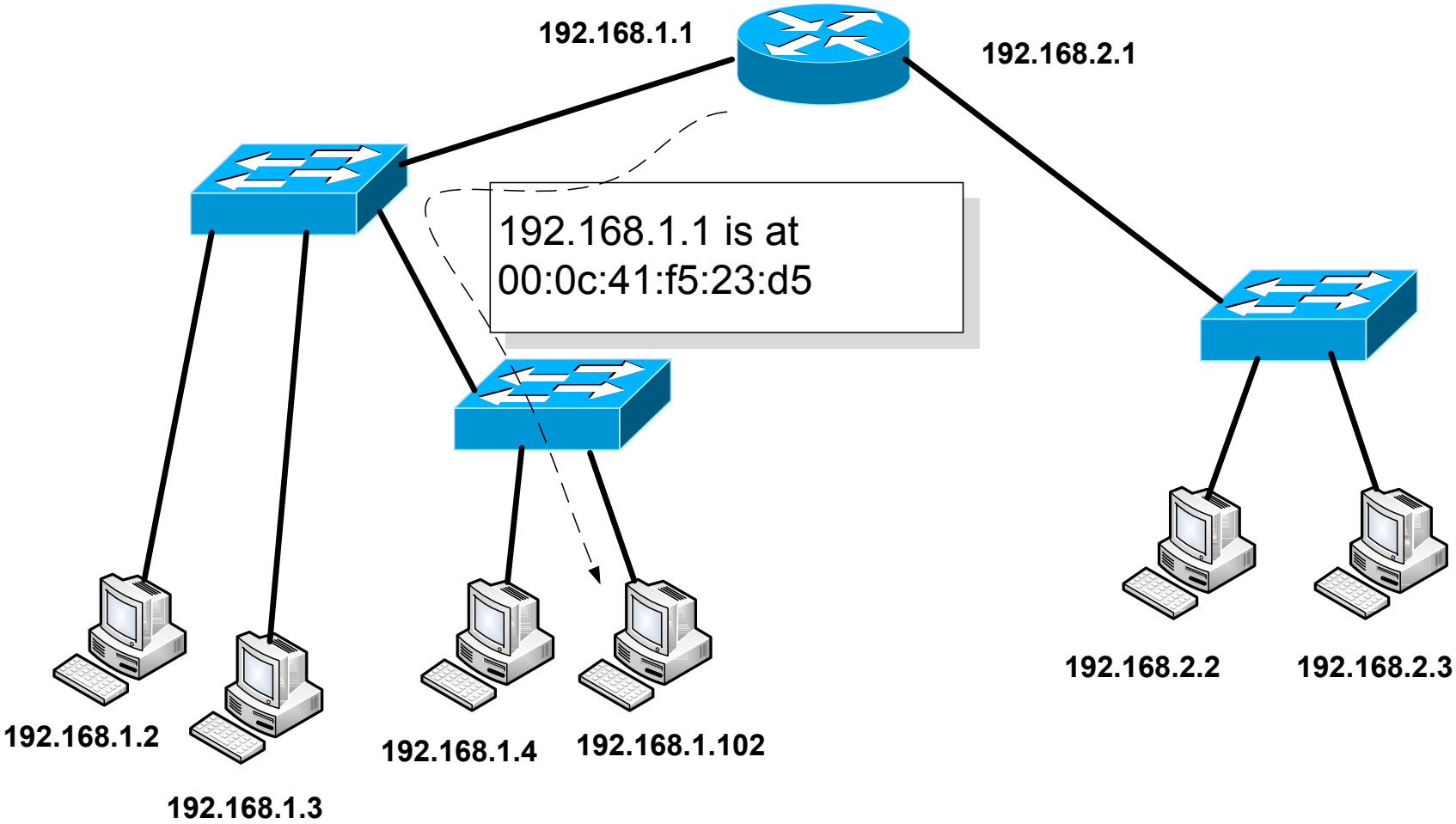
Arp.opcode

Author: Prof Bill Buchanan



ARP

Author: Prof Bill Buchanan



Analysis

Forensic

ARP

Author: Prof Bill Buchanan

capture1 - Ethereal

File Edit View Go Capture Analyze Statistics Help

Filter: Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
7	2.460794	192.168.1.1	239.255.255.250	SSDP	NOTIFY * HTTP/1.1
8	2.461366	192.168.1.1	239.255.255.250	SSDP	NOTIFY * HTTP/1.1
9	2.462065	192.168.1.1	239.255.255.250	SSDP	NOTIFY * HTTP/1.1
10	2.462857	192.168.1.1	239.255.255.250	SSDP	NOTIFY * HTTP/1.1
11	2.463440	192.168.1.1	239.255.255.250	SSDP	NOTIFY * HTTP/1.1
12	3.180406	192.168.1.102	Broadcast	ARP	Who has 192.168.1.1? Tell 192.168.1.102
13	3.196684	192.168.1.1	192.168.1.102	ARP	192.168.1.1 is at 00:0c:41:f5:23:d5
14	3.196693	192.168.1.102	195.92.195.94	DNS	Standard query PTR 250.255.255.239.in-addr.arpa
15	3.253824	195.92.195.94	192.168.1.102	DNS	Standard query response, No such name
16	3.940487	192.168.1.102	195.92.195.94	DNS	Standard query PTR 102.1.168.192.in-addr.arpa

```
⊞ Frame 12 (42 bytes on wire, 42 bytes captured)
⊟ Ethernet II, Src: 192.168.1.102 (00:15:00:34:02:f0), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
    Destination: Broadcast (ff:ff:ff:ff:ff:ff)
    Source: 192.168.1.102 (00:15:00:34:02:f0)
    Type: ARP (0x0806)
⊟ Address Resolution Protocol (request)
    Hardware type: Ethernet (0x0001)
    Protocol type: IP (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (0x0001)
    Sender MAC address: 192.168.1.102 (00:15:00:34:02:f0)
    Sender IP address: 192.168.1.102 (192.168.1.102)
    Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
    Target IP address: 192.168.1.1 (192.168.1.1)

0000  ff ff ff ff ff ff 00 15  00 34 02 f0 08 06 00 01   ........ .4......
0010  08 00 06 04 00 01 00 15  00 34 02 f0 c0 a8 01 66   ........ .4.....f
0020  00 00 00 00 00 00 c0 a8  01 01                     ........ ..
```

File: "c:\capture1" 773 KB 00:05:00 | P: 1108 D: 1108 M: 0

Analysis

Forensic

ARP

Author: Prof Bill Buchanan

capture1 - Ethereal

File Edit View Go Capture Analyze Statistics Help

Filter: Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
7	2.460794	192.168.1.1	239.255.255.250	SSDP	NOTIFY * HTTP/1.1
8	2.461366	192.168.1.1	239.255.255.250	SSDP	NOTIFY * HTTP/1.1
9	2.462065	192.168.1.1	239.255.255.250	SSDP	NOTIFY * HTTP/1.1
10	2.462857	192.168.1.1	239.255.255.250	SSDP	NOTIFY * HTTP/1.1
11	2.463440	192.168.1.1	239.255.255.250	SSDP	NOTIFY * HTTP/1.1
12	3.180406	192.168.1.102	Broadcast	ARP	Who has 192.168.1.1? Tell 192.168.1.102
13	3.196684	192.168.1.1	192.168.1.102	ARP	192.168.1.1 is at 00:0c:41:f5:23:d5
14	3.196693	192.168.1.102	195.92.195.94	DNS	Standard query PTR 250.255.255.239.in-addr.arpa
15	3.253824	195.92.195.94	192.168.1.102	DNS	Standard query response, No such name
16	3.940487	192.168.1.102	195.92.195.94	DNS	Standard query PTR 102.1.168.192.in-addr.arpa

```
Frame 13 (60 bytes on wire, 60 bytes captured)
Ethernet II, Src: 192.168.1.1 (00:0c:41:f5:23:d5), Dst: 192.168.1.102 (00:15:00:34:02:f0)
    Destination: 192.168.1.102 (00:15:00:34:02:f0)
    Source: 192.168.1.1 (00:0c:41:f5:23:d5)
    Type: ARP (0x0806)
    Trailer: 901EFC775018FE759DA000002A204C495354
Address Resolution Protocol (reply)
    Hardware type: Ethernet (0x0001)
    Protocol type: IP (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (0x0002)
    Sender MAC address: 192.168.1.1 (00:0c:41:f5:23:d5)
    Sender IP address: 192.168.1.1 (192.168.1.1)
    Target MAC address: 192.168.1.102 (00:15:00:34:02:f0)
```

```
0000  00 15 00 34 02 f0 00 0c  41 f5 23 d5 08 06 00 01   ...4.... A.#.....
0010  08 00 06 04 00 02 00 0c  41 f5 23 d5 c0 a8 01 01   ........ A.#.....
0020  00 15 00 34 02 f0 c0 a8  01 66 90 1e fc 77 50 18   ...4.... .f...wP.
0030  fe 75 9d a0 00 00 2a 20  4c 49 53 54               .u....*  LIST
```

Hardware size (arp.hw.size), 1 byte | P: 1108 D: 1108 M: 0

Analysis

Forensic

ARP

Author: Prof Bill Buchanan

capture1 - Ethereal

File Edit View Go Capture Analyze Statistics Help

Filter: icmp.type Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
945	67.238974	192.168.1.102	66.102.9.104	ICMP	Echo (ping) request
946	67.284001	66.102.9.104	192.168.1.102	ICMP	Echo (ping) reply
947	68.240072	192.168.1.102	66.102.9.104	ICMP	Echo (ping) request
948	68.301073	66.102.9.104	192.168.1.102	ICMP	Echo (ping) reply
949	69.241058	192.168.1.102	66.102.9.104	ICMP	Echo (ping) request
950	69.302003	66.102.9.104	192.168.1.102	ICMP	Echo (ping) reply
951	70.242048	192.168.1.102	66.102.9.104	ICMP	Echo (ping) request
952	70.302754	66.102.9.104	192.168.1.102	ICMP	Echo (ping) reply

```
⊞ Frame 945 (74 bytes on wire, 74 bytes captured)
⊞ Ethernet II, Src: 192.168.1.102 (00:15:00:34:02:f0), Dst: 192.168.1.1 (00:0c:41:f5:23:d5)
⊞ Internet Protocol, Src: 192.168.1.102 (192.168.1.102), Dst: 66.102.9.104 (66.102.9.104)
⊟ Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x455c [correct]
    Identifier: 0x0200
    Sequence number: 0x0600
    Data (32 bytes)

0000  00 0c 41 f5 23 d5 00 15  00 34 02 f0 08 00 45 00   ..A.#... .4....E.
0010  00 3c 0a 60 00 00 80 01  22 85 c0 a8 01 66 42 66   .<.`.... "....fBf
0020  09 68 08 00 45 5c 02 00  06 00 61 62 63 64 65 66   .h..E\.. ..abcdef
0030  67 68 69 6a 6b 6c 6d 6e  6f 70 71 72 73 74 75 76   ghijklmn opqrstuv
0040  77 61 62 63 64 65 66 67  68 69                     wabcdefg hi
```

Forensic Analysis

ICMP.type

Author: Prof Bill Buchanan

capture1 - Ethereal

File Edit View Go Capture Analyze Statistics Help

Filter: icmp.type Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
945	67.238974	192.168.1.102	66.102.9.104	ICMP	Echo (ping) request
946	67.284001	66.102.9.104	192.168.1.102	ICMP	Echo (ping) reply
947	68.240072	192.168.1.102	66.102.9.104	ICMP	Echo (ping) request
948	68.301073	66.102.9.104	192.168.1.102	ICMP	Echo (ping) reply
949	69.241058	192.168.1.102	66.102.9.104	ICMP	Echo (ping) request
950	69.302003	66.102.9.104	192.168.1.102	ICMP	Echo (ping) reply
951	70.242048	192.168.1.102	66.102.9.104	ICMP	Echo (ping) request
952	70.302754	66.102.9.104	192.168.1.102	ICMP	Echo (ping) reply

```
⊞ Frame 946 (74 bytes on wire, 74 bytes captured)
⊞ Ethernet II, Src: 192.168.1.1 (00:0c:41:f5:23:d5), Dst: 192.168.1.102 (00:15:00:34:02:f0)
⊞ Internet Protocol, Src: 66.102.9.104 (66.102.9.104), Dst: 192.168.1.102 (192.168.1.102)
⊟ Internet Control Message Protocol
    Type: 0 (Echo (ping) reply)
    Code: 0
    Checksum: 0x4d5c [correct]
    Identifier: 0x0200
    Sequence number: 0x0600
    Data (32 bytes)
```

```
0000  00 15 00 34 02 f0 00 0c  41 f5 23 d5 08 00 45 00   ...4.... A.#...E.
0010  00 3c 0a 60 00 00 f6 01  ac 84 42 66 09 68 c0 a8   .<.`.... ..Bf.h..
0020  01 66 00 00 4d 5c 02 00  06 00 61 62 63 64 65 66   .f..M\.. ..abcdef
0030  67 68 69 6a 6b 6c 6d 6e  6f 70 71 72 73 74 75 76   ghijklmn opqrstuv
0040  77 61 62 63 64 65 66 67  68 69                     wabcdefg hi
```

Forensi

ICMP.type

Author: Prof Bill Buchanan

capture1 - Ethereal

File Edit View Go Capture Analyze Statistics Help

Filter: http.request.method=="GET" Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
34	15.703799	192.168.1.102	66.102.9.147	HTTP	GET / HTTP/1.1
99	26.872927	192.168.1.102	66.102.9.147	HTTP	GET /search?hl=en&q=napier+university+research&meta= HTTP/1
127	40.516290	192.168.1.102	66.102.9.147	HTTP	GET /url?sa=T&ct=res&cd=1&url=http%3A%2F%2Fwww.tri.napier.a
138	40.855081	192.168.1.102	146.176.1.121	HTTP	GET / HTTP/1.1
141	41.111071	192.168.1.102	146.176.1.121	HTTP	GET /Fonts/LinkNotUnderlined.css HTTP/1.1
156	41.246320	192.168.1.102	146.176.1.121	HTTP	GET /images_about/tunnel_pic.jpg HTTP/1.1
159	41.249030	192.168.1.102	146.176.1.121	HTTP	GET /images_about/about_us.gif HTTP/1.1
161	41.308425	192.168.1.102	146.176.1.121	HTTP	GET /images_about/left_spacer.gif HTTP/1.1
163	41.322293	192.168.1.102	146.176.1.121	HTTP	GET /images_about/members.gif HTTP/1.1
165	41.360616	192.168.1.102	146.176.1.121	HTTP	GET /images_about/research.gif HTTP/1.1

```
⊞ Frame 34 (371 bytes on wire, 371 bytes captured)
⊟ Ethernet II, Src: 192.168.1.102 (00:15:00:34:02:f0), Dst: 192.168.1.1 (00:0c:41:f5:23:d5)
    Destination: 192.168.1.1 (00:0c:41:f5:23:d5)
    Source: 192.168.1.102 (00:15:00:34:02:f0)
    Type: IP (0x0800)
⊞ Internet Protocol, Src: 192.168.1.102 (192.168.1.102), Dst: 66.102.9.147 (66.102.9.147)
⊟ Transmission Control Protocol, Src Port: 1386 (1386), Dst Port: http (80), Seq: 1, Ack: 1, Len: 317
    Source port: 1386 (1386)
    Destination port: http (80)
    Sequence number: 1    (relative sequence number)
    [Next sequence number: 318    (relative sequence number)]
    Acknowledgement number: 1    (relative ack number)
    Header length: 20 bytes
  ⊞ Flags: 0x0018 (PSH, ACK)
    Window size: 17640
```

```
0000  00 0c 41 f5 23 d5 00 15  00 34 02 f0 08 00 45 00   ..A.#... .4....E.
0010  01 65 07 58 40 00 80 06  e4 33 c0 a8 01 66 42 66   .e.X@... .3...fBf
0020  09 93 05 6a 00 50 eb de  bb 4b 79 e0 18 00 50 18   ...j.P.. .Ky...P.
0030  44 e8 2b 7f 00 00 47 45  54 20 2f 20 48 54 54 50   D.+...GE T / HTTP
0040  2f 31 2e 31 0d 0a 41 63  63 65 70 74 3a 20 2a 2f   /1.1..Ac cept: */
0050  2a 0d 0a 41 63 63 65 70  74 2d 4c 61 6e 67 75 61   *..Accep t-Langua
0060  67 65 3a 20 65 6e 2d 67  62 0d 0a 55 41 2d 43 50   ge: en-g b..UA-CP
0070  55 3a 20 78 38 36 0d 0a  41 63 63 65 70 74 2d 45   U: x86.. Accept-E
0080  6e 63 6f 64 69 6e 67 3a  20 67 7a 69 70 2c 20 64   ncoding: gzip, d
```

File: "c:\capture1" 773 KB 00:05:00 | P: 1108 D: 28 M: 0

Analysis

Forensic

Http.request.method==”GET”

Author: Prof Bill Buchanan

capture1 - Ethereal

File Edit View Go Capture Analyze Statistics Help

Filter: http.request.method!="GET" Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
9	2.462065	192.168.1.1	239.255.255.250	SSDP	NOTIFY * HTTP/1.1
10	2.462857	192.168.1.1	239.255.255.250	SSDP	NOTIFY * HTTP/1.1
11	2.463440	192.168.1.1	239.255.255.250	SSDP	NOTIFY * HTTP/1.1
45	16.275998	192.168.1.102	131.107.113.76	HTTP	POST /sqm/ie/sqmserver.dll HTTP/1.1 (application/octet-stre
60	16.811655	192.168.1.102	131.107.113.76	HTTP	POST /sqm/ie/sqmserver.dll HTTP/1.1 (application/octet-stre
75	17.504991	192.168.1.102	131.107.113.76	HTTP	POST /sqm/ie/sqmserver.dll HTTP/1.1 (application/octet-stre
90	18.119891	192.168.1.102	131.107.113.76	HTTP	POST /sqm/ie/sqmserver.dll HTTP/1.1 (application/octet-stre
116	33.484474	192.168.1.1	239.255.255.250	SSDP	NOTIFY * HTTP/1.1
117	33.484790	192.168.1.1	239.255.255.250	SSDP	NOTIFY * HTTP/1.1
118	33.485646	192.168.1.1	239.255.255.250	SSDP	NOTIFY * HTTP/1.1

```
⊞ Frame 45 (662 bytes on wire, 662 bytes captured)
⊟ Ethernet II, Src: 192.168.1.102 (00:15:00:34:02:f0), Dst: 192.168.1.1 (00:0c:41:f5:23:d5)
    Destination: 192.168.1.1 (00:0c:41:f5:23:d5)
    Source: 192.168.1.102 (00:15:00:34:02:f0)
    Type: IP (0x0800)
⊞ Internet Protocol, Src: 192.168.1.102 (192.168.1.102), Dst: 131.107.113.76 (131.107.113.76)
⊟ Transmission Control Protocol, Src Port: 1387 (1387), Dst Port: http (80), Seq: 433, Ack: 1, Len: 608
    Source port: 1387 (1387)
    Destination port: http (80)
    Sequence number: 433    (relative sequence number)
    [Next sequence number: 1041    (relative sequence number)]
    Acknowledgement number: 1    (relative ack number)
    Header length: 20 bytes
  ⊞ Flags: 0x0018 (PSH, ACK)
    Window size: 17640
```

```
0000  00 0c 41 f5 23 d5 00 15  00 34 02 f0 08 00 45 00   ..A.#... .4....E.
0010  02 88 07 5f 40 00 80 06  3a 4b c0 a8 01 66 83 6b   ..._@... :K...f.k
0020  71 4c 05 6b 00 50 43 a3  cd e6 22 27 2d d8 50 18   qL.k.PC. .."'-.P.
0030  44 e8 c3 6a 00 00 4d 53  51 4d 78 00 00 00 00 00   D..j..MS QMx.....
0040  00 00 d0 89 15 12 03 00  00 00 e8 01 00 00 00 00   ........ ........
0050  00 00 00 00 00 00 00 00  00 00 00 00 00 00 60 4f   ........ ......`O
```

Frame (662 bytes) | Reassembled TCP (1040 bytes)

File: "c:\capture1" 773 KB 00:05:00 | P: 1108 D: 104 M: 0

Forensi

Http.request.method!=”GET”

Author: Prof Bill Buchanan

seg1 - Ethereal

File Edit View Go Capture Analyze Statistics Help

Filter: ftp.request.command=="USER" Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
28321	290.613568	44.16.113.50	10.0.1.69	FTP	Request: USER anonymous
30389	309.711793	68.37.75.158	10.0.1.148	FTP	Request: USER anonymous
44803	451.299916	66.7.248.153	10.0.1.148	FTP	Request: USER anonymous
65656	634.070352	68.37.75.158	10.0.1.148	FTP	Request: USER anonymous
69504	669.595091	44.16.113.50	10.0.1.69	FTP	Request: USER anonymous
75088	745.452837	66.27.251.21	10.0.1.148	FTP	Request: USER anonymous
82560	863.403952	66.27.251.21	10.0.1.148	FTP	Request: USER anonymous
87004	915.406069	67.73.151.50	10.0.1.148	FTP	Request: USER anonymous
87471	921.677631	67.73.151.50	10.0.1.148	FTP	Request: USER anonymous
87890	927.690212	67.115.218.108	10.0.1.148	FTP	Request: USER anonymous
87898	927.709866	66.27.251.21	10.0.1.148	FTP	Request: USER anonymous
89170	942.364409	67.115.218.108	10.0.1.148	FTP	Request: USER anonymous

```
⊞ Frame 28321 (70 bytes on wire, 70 bytes captured)
⊟ Ethernet II, Src: Cisco_04:41:bc (00:00:0c:04:41:bc), Dst: 10.0.1.1 (00:0c:ce:85:ab:60)
    Destination: 10.0.1.1 (00:0c:ce:85:ab:60)
    Source: Cisco_04:41:bc (00:00:0c:04:41:bc)
    Type: IP (0x0800)
⊞ Internet Protocol, Src: 44.16.113.50 (44.16.113.50), Dst: 10.0.1.69 (10.0.1.69)
⊟ Transmission Control Protocol, Src Port: 1026 (1026), Dst Port: ftp (21), Seq: 1, Ack: 96, Len: 16
    Source port: 1026 (1026)
    Destination port: ftp (21)
    Sequence number: 1    (relative sequence number)
    [Next sequence number: 17    (relative sequence number)]
    Acknowledgement number: 96    (relative ack number)
    Header length: 20 bytes
  ⊞ Flags: 0x0018 (PSH, ACK)
    Window size: 4096
    Checksum: 0x5b1f [correct]
⊟ File Transfer Protocol (FTP)
  ⊟ USER anonymous\r\n
      Request command: USER
      Request arg: anonymous
```

```
0000  00 0c ce 85 ab 60 00 00  0c 04 41 bc 08 00 45 00   .....`.. ..A...E.
0010  00 38 07 85 00 00 3b 06  cf b4 2c 10 71 32 0a 00   .8....;. ..,.q2..
0020  01 45 04 02 00 15 2d 57  6c 02 67 a2 0f 27 50 18   .E....-W l.g..'P.
0030  10 00 5b 1f 00 00 55 53  45 52 20 61 6e 6f 6e 79   ..[...US ER anony
0040  6d 6f 75 73 0d 0a                                  mous..
```

Analysis

Forensic

Ftp.request.command==”USER”

Author: Prof Bill Buchanan

seg1 - Ethereal

File Edit View Go Capture Analyze Statistics Help

Filter: ftp.request.command!="USER" Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
28323	290.614229	44.16.113.50	10.0.1.69	FTP	Request: PASS avrap@zeno.eyrie.af.mil
28325	290.615675	44.16.113.50	10.0.1.69	FTP	Request: PORT 172,16,113,50,4,3
28326	290.616098	44.16.113.50	10.0.1.69	FTP	Request: NLST
28332	290.635457	44.16.113.50	10.0.1.69	FTP	Request: CWD mailing_list
28334	290.636110	44.16.113.50	10.0.1.69	FTP	Request: PORT 172,16,113,50,4,4
28335	290.636926	44.16.113.50	10.0.1.69	FTP	Request: NLST
28341	290.655277	44.16.113.50	10.0.1.69	FTP	Request: CWD archive
28343	290.655993	44.16.113.50	10.0.1.69	FTP	Request: PORT 172,16,113,50,4,5
28344	290.656401	44.16.113.50	10.0.1.69	FTP	Request: NLST
28351	290.677156	44.16.113.50	10.0.1.69	FTP	Request: CWD music
28353	290.696676	44.16.113.50	10.0.1.69	FTP	Request: PORT 172,16,113,50,4,6
28354	290.697127	44.16.113.50	10.0.1.69	FTP	Request: NLST

```
⊞ Frame 28325 (78 bytes on wire, 78 bytes captured)
⊟ Ethernet II, Src: Cisco_04:41:bc (00:00:0c:04:41:bc), Dst: 10.0.1.1 (00:0c:ce:85:ab:60)
    Destination: 10.0.1.1 (00:0c:ce:85:ab:60)
    Source: Cisco_04:41:bc (00:00:0c:04:41:bc)
    Type: IP (0x0800)
⊞ Internet Protocol, Src: 44.16.113.50 (44.16.113.50), Dst: 10.0.1.69 (10.0.1.69)
⊟ Transmission Control Protocol, Src Port: 1026 (1026), Dst Port: ftp (21), Seq: 47, Ack: 212, Len: 24
    Source port: 1026 (1026)
    Destination port: ftp (21)
    Sequence number: 47    (relative sequence number)
    [Next sequence number: 71    (relative sequence number)]
    Acknowledgement number: 212    (relative ack number)
    Header length: 20 bytes
  ⊞ Flags: 0x0018 (PSH, ACK)
    Window size: 4096
    Checksum: 0x86ee [correct]
⊟ File Transfer Protocol (FTP)
  ⊟ PORT 172,16,113,50,4,3\r\n
      Request command: PORT
      Request arg: 172,16,113,50,4,3
      Active IP address: 172.16.113.50 (172.16.113.50)
      Active port: 1027
      Active IP NAT: True
```

```
0000  00 0c ce 85 ab 60 00 00  0c 04 41 bc 08 00 45 00   .....`.. ..A...E.
0010  00 40 07 92 00 00 3b 06  cf 9f 2c 10 71 32 0a 00   .@....;. ..,.q2..
0020  01 45 04 02 00 15 2d 57  6c 30 67 a2 0f 9b 50 18   .E....-W l0g...P.
0030  10 00 86 ee 00 00 50 4f  52 54 20 31 37 32 2c 31   ......PO RT 172,1
0040  36 2c 31 31 33 2c 35 30  2c 34 2c 33 0d 0a          6,113,50 ,4,3..
```

Forens

Ftp.request.command!=”USER”

Author: Prof Bill Buchanan

capture1 - Ethereal

File Edit View Go Capture Analyze Statistics Help

Filter: Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
17	3.940580	192.168.1.102	195.92.195.94	DNS	Standard query PTR 94.195.92.195.in-addr.arpa
18	3.983040	195.92.195.94	192.168.1.102	DNS	Standard query response, No such name
19	3.984345	195.92.195.94	192.168.1.102	DNS	Standard query response PTR resolver1.svr.pol.co.uk
20	4.704158	192.168.1.102	195.92.195.94	DNS	Standard query A resolver1.svr.pol.co.uk
21	4.757633	195.92.195.94	192.168.1.102	DNS	Standard query response A 195.92.195.94
22	5.443409	192.168.1.102	195.92.195.95	DNS	Standard query PTR 1.1.168.192.in-addr.arpa
23	5.496852	195.92.195.95	192.168.1.102	DNS	Standard query response, No such name
24	6.197343	192.168.1.102	195.92.195.94	DNS	Standard query PTR 95.195.92.195.in-addr.arpa
25	6.239212	195.92.195.94	192.168.1.102	DNS	Standard query response PTR resolver2.svr.pol.co.uk
26	6.944430	192.168.1.102	195.92.195.94	DNS	Standard query A resolver2.svr.pol.co.uk
27	6.993211	195.92.195.94	192.168.1.102	DNS	Standard query response A 195.92.195.95
28	15.617521	192.168.1.102	195.92.195.94	DNS	Standard query A www.google.co.uk
29	15.657133	195.92.195.94	192.168.1.102	DNS	Standard query response CNAME www.google.com CNAME www.l.google.com A 66.102.9.
30	15.658058	192.168.1.102	66.102.9.147	TCP	1386 > http [SYN] Seq=0 Ack=0 Win=16384 Len=0 MSS=1260
31	15.660307	192.168.1.1	192.168.1.255	SNMP	TRAP-V1 SNMPv2-SMI::enterprises.39
32	15.703566	66.102.9.147	192.168.1.102	TCP	http > 1386 [SYN, ACK] Seq=0 Ack=1 2
33	15.703606	192.168.1.102	66.102.9.147	TCP	1386 > http [ACK] Seq=1 Ack=1 Win=
34	15.703799	192.168.1.102	66.102.9.147	HTTP	GET / HTTP/1.1
35	15.763432	66.102.9.147	192.168.1.102	TCP	http > 1386 [ACK] Seq=1 Ack=318 Wi
36	15.763837	66.102.9.147	192.168.1.102	TCP	[TCP Window Update] http > 1386 [A 432 Len=0

Mark Packet (toggle)
Time Reference
Apply as Filter
Prepare a Filter
Follow TCP Stream
Decode As...
Print...
Show Packet in New Window

Follow TCP stream

Stream Content

```
...m....3...[}.Oid.~......i..8.....D.4
6_o...n.E.ZU.....9%.
X...XN#cE .n'@^..G"..s.IB...t.1.
f-..>....3F.:.vR.+Y..!f....].~c.....wHQ..8.oE..O.......?<_...'2c.M....@z..fm.\.%S..:..,
>...D..&.....]
`..v(z.6..;l.%+g..q....5:.........<.......7....*r........6.(U...)...F......b|...OJ.N.w.
..:..5a1.Y...;...{.m.^j....Jg@..8.....Q.M1.......".........&.?f'.O.d.y...[.S..."H... .Q
......Ik.,$uw...^..E...Q.......X3..#z.....t.mr.....r!..3..I3_.1...E..N,.j......B...M..1
9d
..y..Q...P.e..rN1".YG.:.6...:3...
. :.P%.).@e.).....2ho...J37...C....Ee.....vN.@....nz~.dt.]-x..$....^.e.".cO..p*.SK./..
0

GET /url?sa=T&ct=res&cd=1&url=http%3A%2F%2Fwww.tri.napier.ac.uk%2F&ei=wqVLRI6RCcjuRdihq
Accept: */*
Referer: http://www.google.co.uk/search?hl=en&q=napier+university+research&meta=
Accept-Language: en-gb
UA-CPU: x86
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322)
Host: www.google.co.uk
Connection: Keep-Alive
Cookie: PREF=ID=5885260b4cb19112:TM=1145537782:LM=1145537782:S=B7-bR8IBtNJ83VFt

HTTP/1.1 204 No Content
Cache-Control: private
Content-Type: text/html
Server: GWS/2.1
Content-Length: 0
Date: Sun, 23 Apr 2006 16:05:35 GMT
```

Save As | Print | Entire conversation (8648 bytes) | ASCII | EBCDIC | Hex Dump | C Arrays | Raw

Filter out this stream | Close

2.168.2.3

Author: Prof Bill Buchanan

Application layer analysis

capture2 - Wireshark

File Edit View Go Capture Analyze Statistics Help

Filter: (ip.addr eq 192.168.1.102 and ip.addr eq 198.1 Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
22	14.616908	192.168.1.102	198.175.98.64	TCP	ms-sql-s > ftp [SYN] Seq=0 Win=16384 Len=0
24	14.965285	198.175.98.64	192.168.1.102	TCP	ftp > ms-sql-s [SYN, ACK] Seq=0 Ack=1 Win=
25	14.965326	192.168.1.102	198.175.98.64	TCP	ms-sql-s > ftp [ACK] Seq=1 Ack=1 Win=17640
26	15.354782	198.175.98.64	192.168.1.102	FTP	Response: 220 ftp1 FTP server (Version wu-
28	15.479338	192.168.1.102	198.175.98.64	TCP	ms-sql-s > ftp [ACK] Seq=1 Ack=63 Win=1757
31	18.429998	192.168.1.102	198.175.98.64	FTP	Request: USER anonymous
32	18.733716	198.175.98.64	192.168.1.102	TCP	ftp > ms-sql-s [ACK] Seq=63 Ack=17 Win=584
33	18.734206	198.175.98.64	192.168.1.102	FTP	Response: 331 Guest login ok, send your co
34	18.901326	192.168.1.102	198.175.98.64	TCP	ms-sql-s > ftp [ACK] Seq=17 Ack=131 Win=17
35	25.438971	192.168.1.102	198.175.98.64	FTP	Request: PASS fred@home
36	25.797929	198.175.98.64	192.168.1.102	FTP	Response: 230-**********
37	25.949360	192.168.1.102	198.175.98.64	TCP	ms-sql-s > ftp [ACK] Seq=33 Ack=198 Win=17
38	26.413369	198.175.98.64	192.168.1.102	FTP	Response: 230-
39	26.552757	192.168.1.102	198.175.98.64	TCP	ms-sql-s > ftp [ACK] Seq=33 Ack=1530 Win=1
40	30.213063	192.168.1.102	198.175.98.64	FTP	Request: PORT 192,168,1,102,5,155
41	30.714505	198.175.98.64	192.168.1.102	FTP	Response: 200 PORT command successful.
42	30.715052	192.168.1.102	198.175.98.64	FTP	Request: LIST

```
Frame 31 (70 bytes on wire, 70 bytes captured)
Ethernet II, Src: IntelCor_34:02:f0 (00:15:00:34:02:f0), Dst: Cisco-Li_f5:23:d5 (00:0c:41:f5:23:d5)
Internet Protocol, Src: 192.168.1.102 (192.168.1.102), Dst: 198.175.98.64 (198.175.98.64)
Transmission Control Protocol, Src Port: ms-sql-s (1433), Dst Port: ftp (21), Seq: 1, Ack: 63, Len: 16
File Transfer Protocol (FTP)
```

```
0000  00 0c 41 f5 23 d5 00 15  00 34 02 f0 08 00 45 00   ..A.#... .4....E.
0010  00 38 26 f3 40 00 80 06  e8 ce c0 a8 01 66 c6 af   .8&.@... .....f..
0020  62 40 05 99 00 15 36 c2  e6 c9 30 87 7f a5 50 18   b@....6. ..0...P.
0030  44 aa 24 d1 00 00 55 53  45 52 20 61 6e 6f 6e 79   D.$...US ER anony
0040  6d 6f 75 73 0d 0a                                  mous..
```

File: "C:\capture2" 21 KB 00:01:08 | Packets: 121 Displayed: 59 Marked: 0 | Profile: Default

Analysis

Forensic

SAMPLE

Author: Prof Bill Buchanan