

# Forensic Video

## Workflow Challenges and Strategies

Gareth Harbord, Senior Digital Forensic Specialist, MPS Video Laboratory

[Gareth.Harbord@met.police.uk](mailto:Gareth.Harbord@met.police.uk)



[Gareth.Harbord@met.police.uk](mailto:Gareth.Harbord@met.police.uk)



# Introduction

Forensic Science - Applying scientific principles and techniques whilst collecting, examining and analysing evidence.

Results should be reliable, repeatable, verifiable.



Gareth.Harbord@met.police.uk



# Introduction

Reliability – Can we trust the results?

Repeatability – Will the same test get the same result?

Verifiability – Can the results be checked?



Gareth.Harbord@met.police.uk



# Contents

- **End State**
- **Video Lab Overview**
- **Diversity of Source and Format**
- **Quantity Not Quality**
- **Acquisition**
- **Ingest**



**METROPOLITAN  
POLICE**

Gareth.Harbord@met.police.uk

NEW  
SCOTLAND  
YARD

# End State – What is it all for?



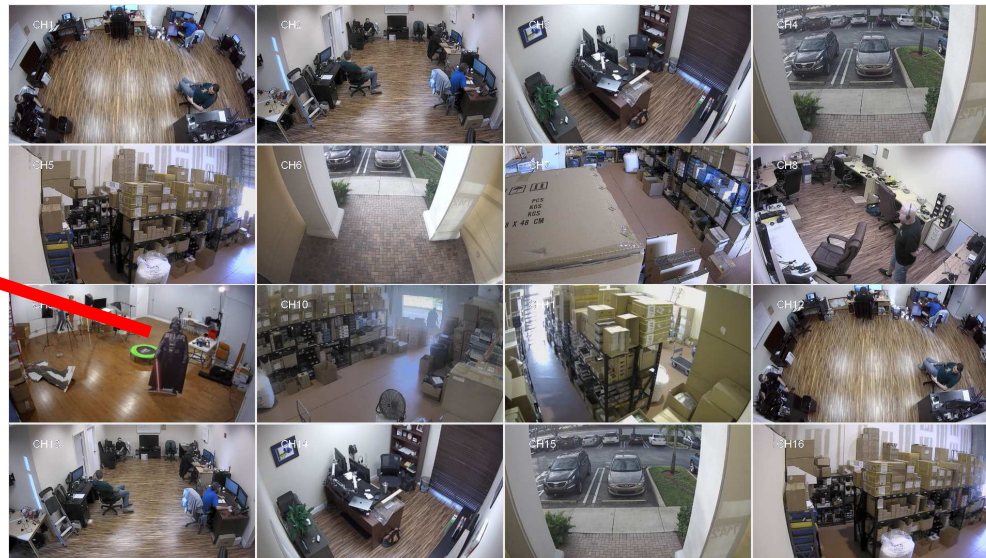
**METROPOLITAN  
POLICE**

Gareth.Harbord@met.police.uk



# End State

- Live Intelligence e.g. tracking a missing person



**METROPOLITAN  
POLICE**

Gareth.Harbord@met.police.uk

**NEW  
SCOTLAND  
YARD**

# End State

- Evidential – Presentation in Court



**METROPOLITAN  
POLICE**

Gareth.Harbord@met.police.uk

NEW  
SCOTLAND  
YARD

# End State

- No Further Action



**METROPOLITAN  
POLICE**

Gareth.Harbord@met.police.uk

NEW  
SCOTLAND  
YARD



# Video Laboratory Overview



**METROPOLITAN  
POLICE**

Gareth.Harbord@met.police.uk



# Video Laboratory Overview

- **Downloads and Data Recovery**
- **Court Compilation/Presentation**
- **Enhancement**
- **Comparison**



**METROPOLITAN  
POLICE**

Gareth.Harbord@met.police.uk



# Video Laboratory Overview

- Downloads and Data Recovery



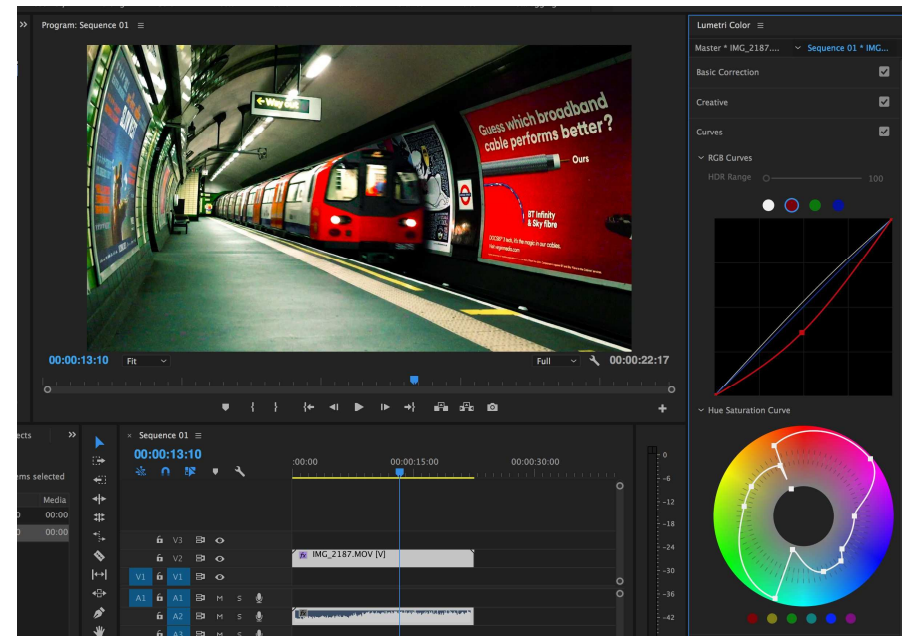
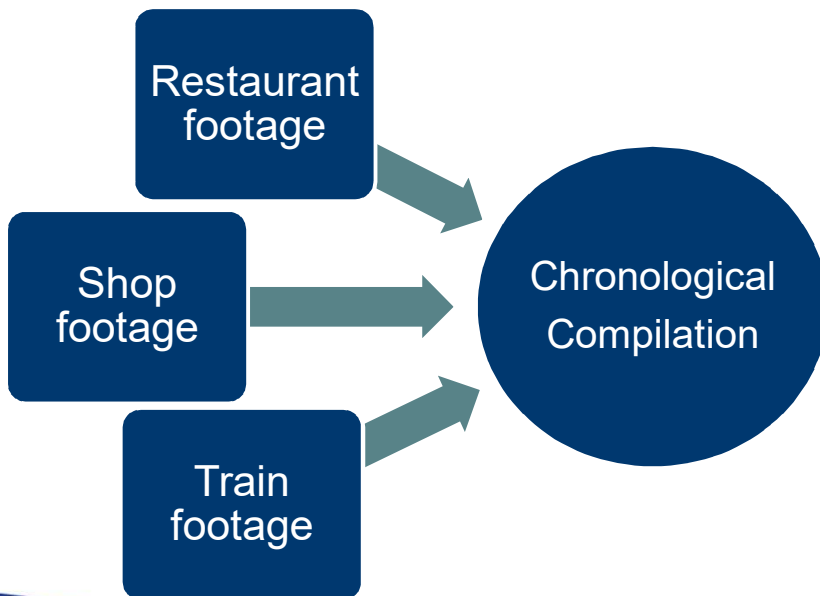
**METROPOLITAN  
POLICE**

Gareth.Harbord@met.police.uk

NEW  
SCOTLAND  
YARD

# Video Laboratory Overview

- Court Compilation/Presentation



# Video Laboratory Overview

- Enhancement



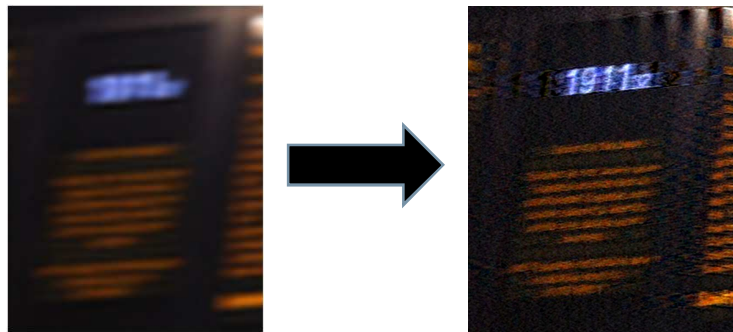
**METROPOLITAN  
POLICE**

Gareth.Harbord@met.police.uk

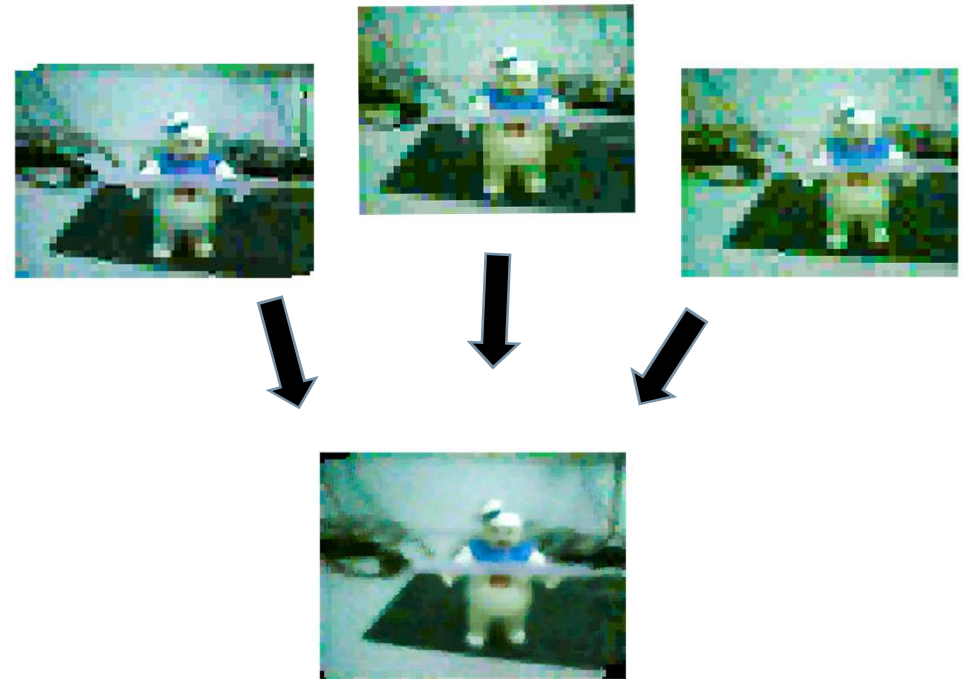
NEW  
SCOTLAND  
YARD

# Video Laboratory Overview

- Enhancement



Blind Deconvolution



Frame Averaging

# Video Laboratory Overview

- Comparison
  - Clothing
  - Facial
  - Objects



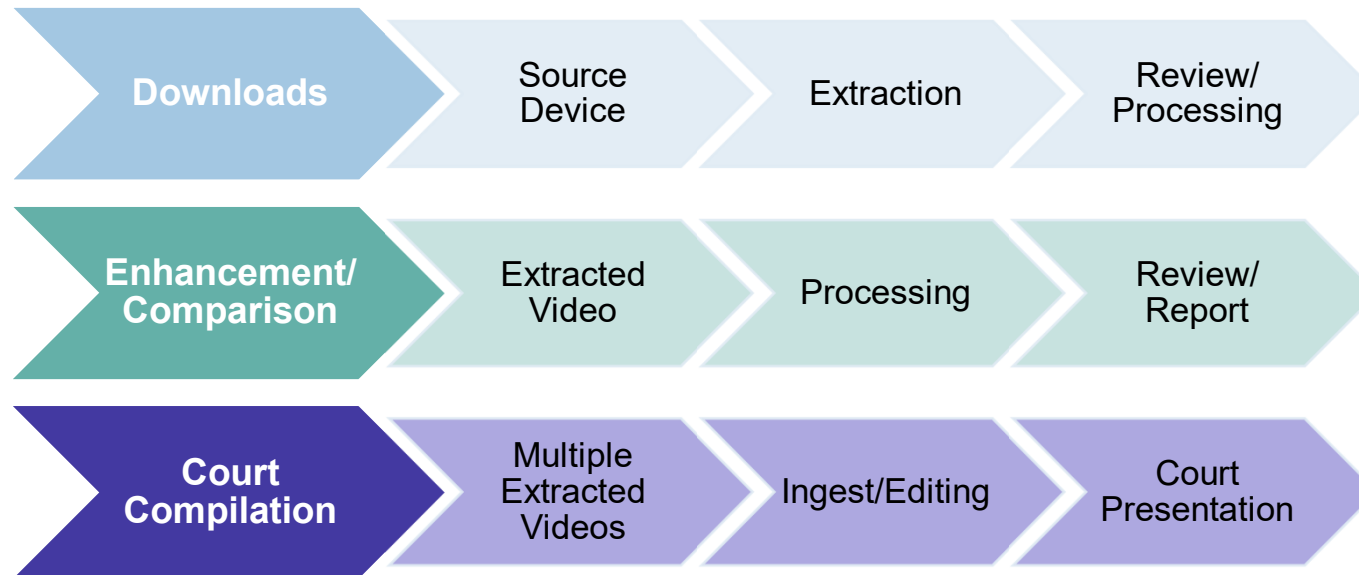
**METROPOLITAN  
POLICE**

Gareth.Harbord@met.police.uk

**NEW  
SCOTLAND  
YARD**

# Video Laboratory Overview

## Overview





# Diversity of source and format



**METROPOLITAN  
POLICE**

Gareth.Harbord@met.police.uk



# Diversity of Source and Format

- CCTV Systems
- IP Cameras
- Network Video Recorder (NVR)
- Digital Video Recorder (DVR)



Gareth.Harbord@met.police.uk



# Diversity of Source and Format

- Mobile Devices



**METROPOLITAN  
POLICE**

Gareth.Harbord@met.police.uk



# Diversity of Source and Format

- Dashboard Cameras



**METROPOLITAN  
POLICE**

Gareth.Harbord@met.police.uk

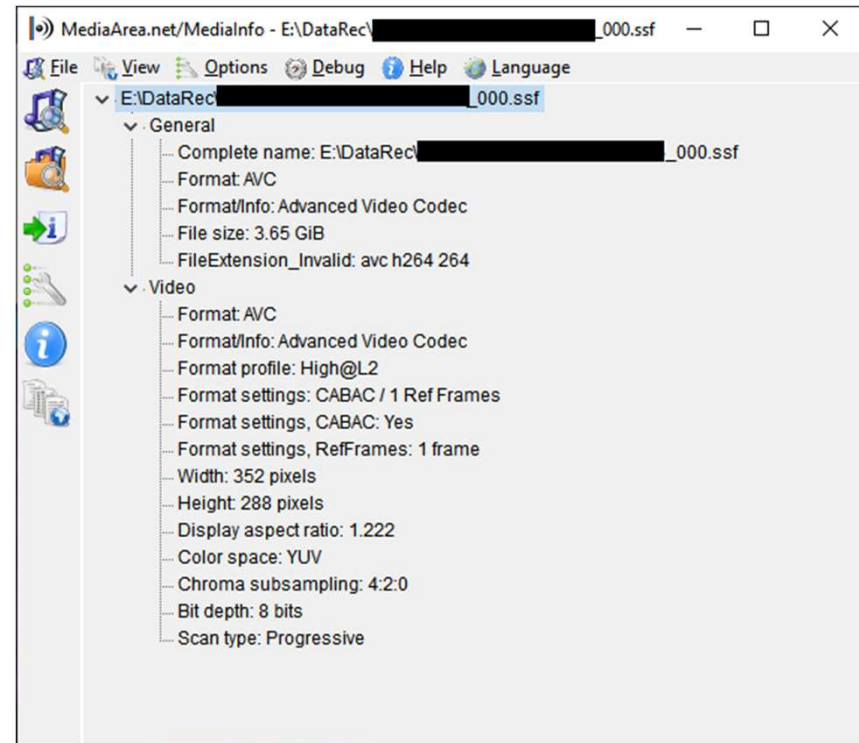
NEW  
SCOTLAND  
YARD

# Diversity of Source and Format

- Diagnostic Tools

Essential!

- MediaInfo
- FFProbe
- ExifTool



<https://mediaarea.net/MediaInfo>

# Diversity of Source and Format

- Legacy analogue formats



U-Matic (3/4")



VHS



8mm, Hi-8, Digital8



Beta SP



Betamax



VHS-C



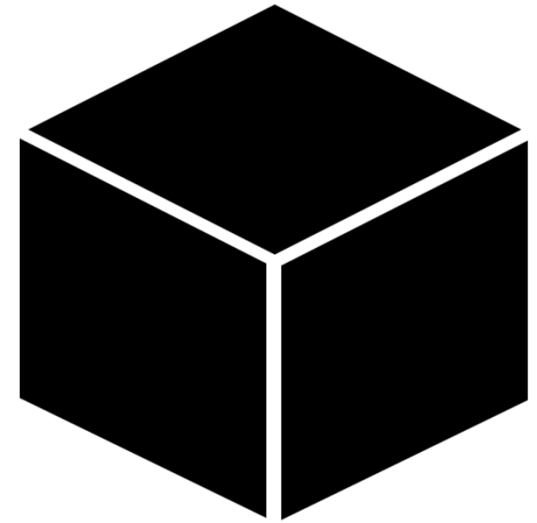
MiniDV



DVCam

# Diversity of Source and Format

- Proprietary codecs
- Proprietary file systems
- Proprietary media containers
- Proprietary replay software
- Unpredictable data integrity



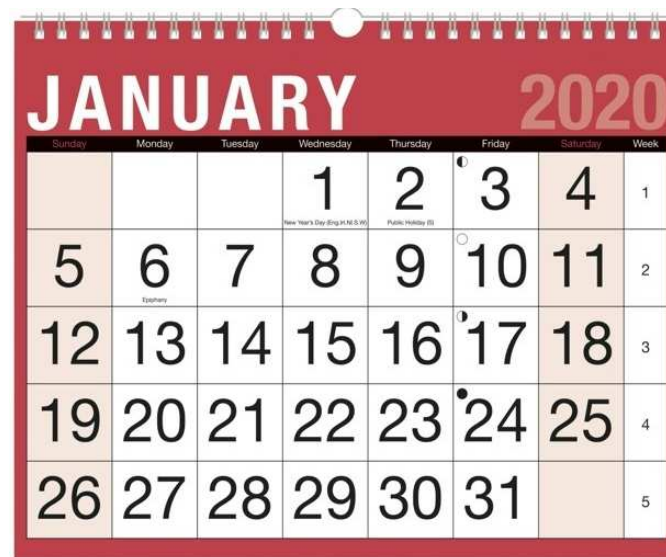
**METROPOLITAN  
POLICE**

Gareth.Harbord@met.police.uk



# Quantity Not Quality

- A 2TB CCTV system may contain 28 days of video



Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday	Week
			1 <small>New Year's Day (Obs. in N.I.S.W.)</small>	2 <small>Public Holiday (I)</small>	3	4	1
5	6 <small>Easter Monday</small>	7	8	9	10	11	2
12	13	14	15	16	17	18	3
19	20	21	22	23	24	25	4
26	27	28	29	30	31		5



**METROPOLITAN  
POLICE**

Gareth.Harbord@met.police.uk





## Quantity Not Quality

- 28 days \* 8 cameras = 5,376 hours!!!
- 5,376 hours on 2TB = 400 kb/s video



**METROPOLITAN  
POLICE**

Gareth.Harbord@met.police.uk

NEW  
SCOTLAND  
YARD

# Quantity Not Quality

Compression at 400 kb/s for HD imagery



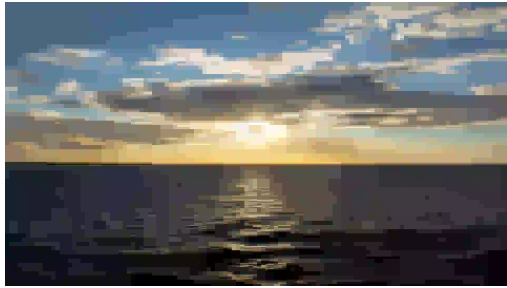
400 kb/s



ORIGINAL

# Quantity Not Quality

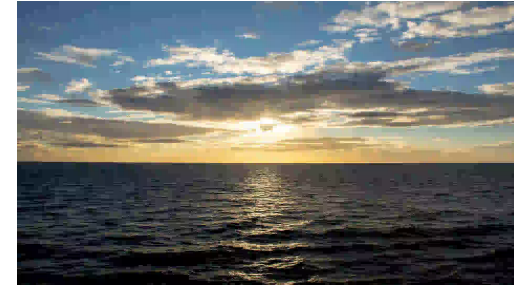
## Bitrate Battles



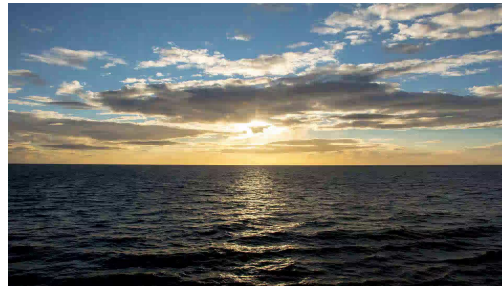
200 kb/s



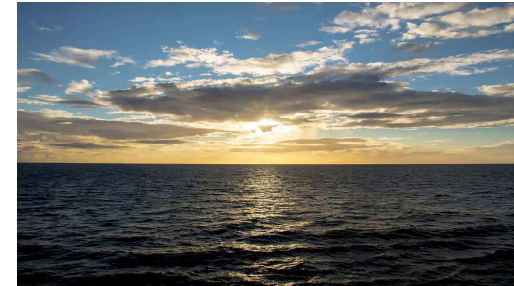
400 kb/s



800 kb/s



2000 kb/s



4000 kb/s



**METROPOLITAN  
POLICE**

Gareth.Harbord@met.police.uk

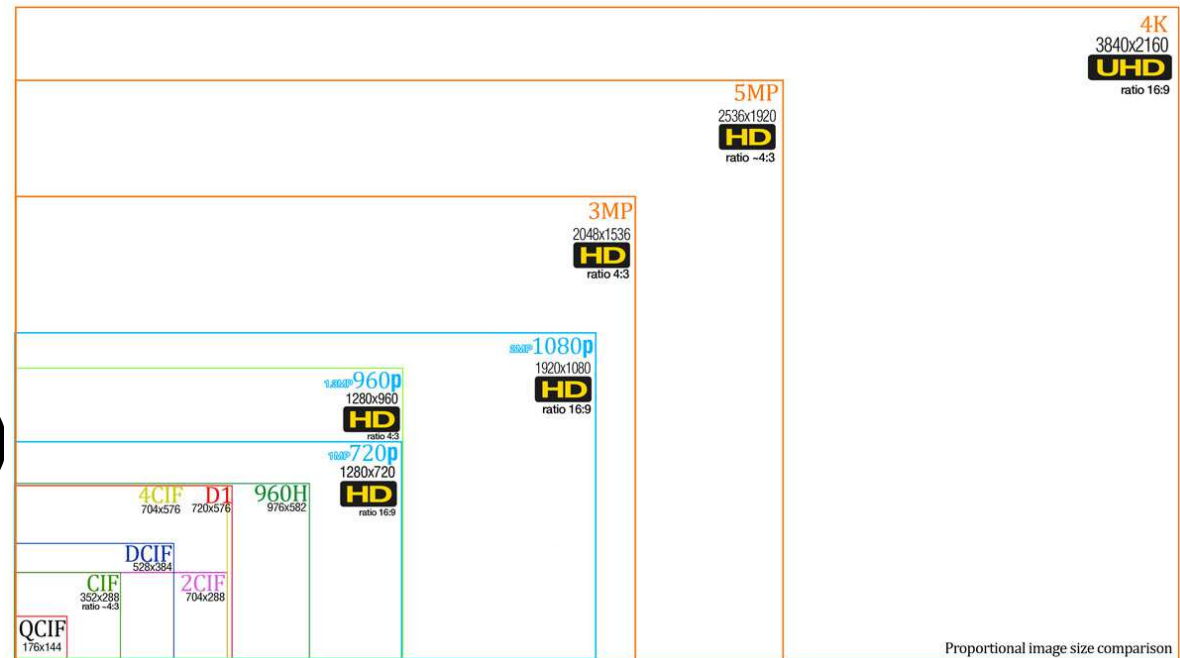


# Quantity Not Quality Resolutions

CIF (352\*240)

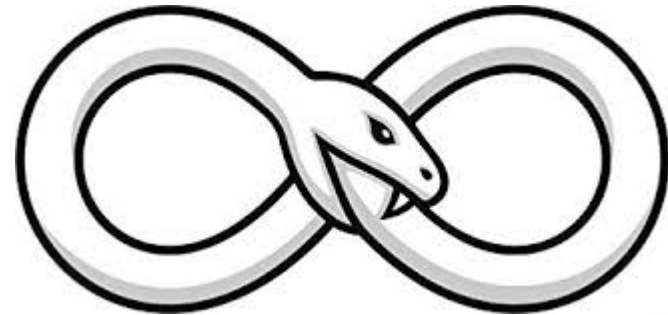


4K (3840\*2160)



## Quantity Not Quality

- Relevant data must be targeted
- Can't keep everything
- Drive clones made by exception
- Quality of source varies greatly
- Constantly overwriting



**METROPOLITAN  
POLICE**

Gareth.Harbord@met.police.uk

NEW  
SCOTLAND  
YARD

# Acquisition



**METROPOLITAN  
POLICE**

Gareth.Harbord@met.police.uk

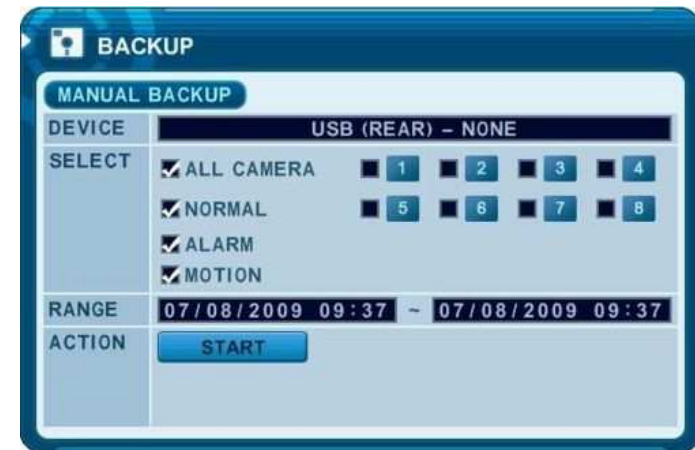


# Acquisition

- Officers try at level 1
- VIIDO try at level 2
- Video Lab at level 3 – toughest 5%
- CCTV presents the biggest challenge
- Hundreds of proprietary file-systems
- Few dedicated extraction tools

# Acquisition

- No format standardization
- Work on the live device
- Disable overwrite
- Native or wrapped?
- Is it there?





# Acquisition

- Legacy hardware can require legacy peripherals
- Hoard your old USB sticks! <2GB



**METROPOLITAN  
POLICE**

Gareth.Harbord@met.police.uk

NEW  
SCOTLAND  
YARD

# The Broken Ones

- Most content sent to the lab is inherently hard to work with.
- Fixes can involve reverse engineering and code generation.
- No single solution.



# Acquisition

- Read media through a write-blocker



# Acquisition

- Use a hex reader

H264 SPS/PPS

Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	ANSI	ASCII
000000000000	68	79	61	76	66	0E	00	00	48	59	41	56	FD	00	02	00	hyavf	HYAVY
000000000016	D8	F2	43	14	D6	02	02	00	8D	06	FA	44	AE	AB	74	17	øòC Ö	úD@«t
000000000032	80	00	76	48	81	00	08	19	00	00	00	00	00	00	00	00	€ vH	
000000000048	00	00	00	01	67	64	00	28	AC	E8	0E	C1	26	40	00	00	gd (-è Á&@	
000000000064	00	01	68	CE	3C	30	00	00	00	01	65	88	82	00	7F	C6	hî<0 e^, Æ	
000000000080	51	C0	CA	00	63	70	4A	98	00	08	38	98	68	8F	57	3C	QÀÊ cpJ~ 8ñ W<	
000000000096	97	84	C6	89	BE	BE	13	BD	4C	3D	FC	CD	91	95	57	7B	-„E%¾¾ ¾L=úÍ `•W{	
000000000112	85	1B	B3	2F	59	86	6D	48	C7	71	20	17	BE	F4	95	6C	... °/YtmHÇq ¾ô•l	
000000000128	A4	22	9F	AB	B6	97	2C	FA	84	30	79	93	B7	F4	3F	8D	π"ž„@— ú 0v" •5?	

# Acquisition

- Collect Samples

Size?

Camera?

00000,	0x	68	79	61	76	66	0E	00	00	48	59	41	56	FD	00	02	00	D8	F2	43	14	D6	02
202D6,	0x	68	79	61	76	D6	02	02	00	48	59	41	56	F0	00	02	04	24	53	55	06	24	08
20AFA,	0x	68	79	61	76	24	08	00	00	48	59	41	56	FC	00	02	08	D9	F2	43	14	F7	17
222F1,	0x	68	79	61	76	F7	17	00	00	48	59	41	56	FC	01	02	08	DA	F2	43	14	D9	12
235CA,	0x	68	79	61	76	D9	12	00	00	48	59	41	56	FC	00	02	08	DB	F2	43	14	02	09
23ECC,	0x	68	79	61	76	02	09	00	00	48	59	41	56	F0	00	02	04	25	53	55	06	24	08
246F0,	0x	68	79	61	76	24	08	00	00	48	59	41	56	FC	01	02	08	DC	F2	43	14	82	09
25072,	0x	68	79	61	76	82	09	00	00	48	59	41	56	FC	00	02	08	DD	F2	43	14	84	08
258F6,	0x	68	79	61	76	84	08	00	00	48	59	41	56	FC	01	02	08	DE	F2	43	14	49	08
2613F,	0x	68	79	61	76	49	08	00	00	48	59	41	56	F0	00	02	04	26	53	55	06	24	08
26963,	0x	68	79	61	76	24	08	00	00	48	59	41	56	FC	00	02	08	DF	F2	43	14	86	08



METROPOLITAN  
POLICE

Gareth.Harbord@met.police.uk





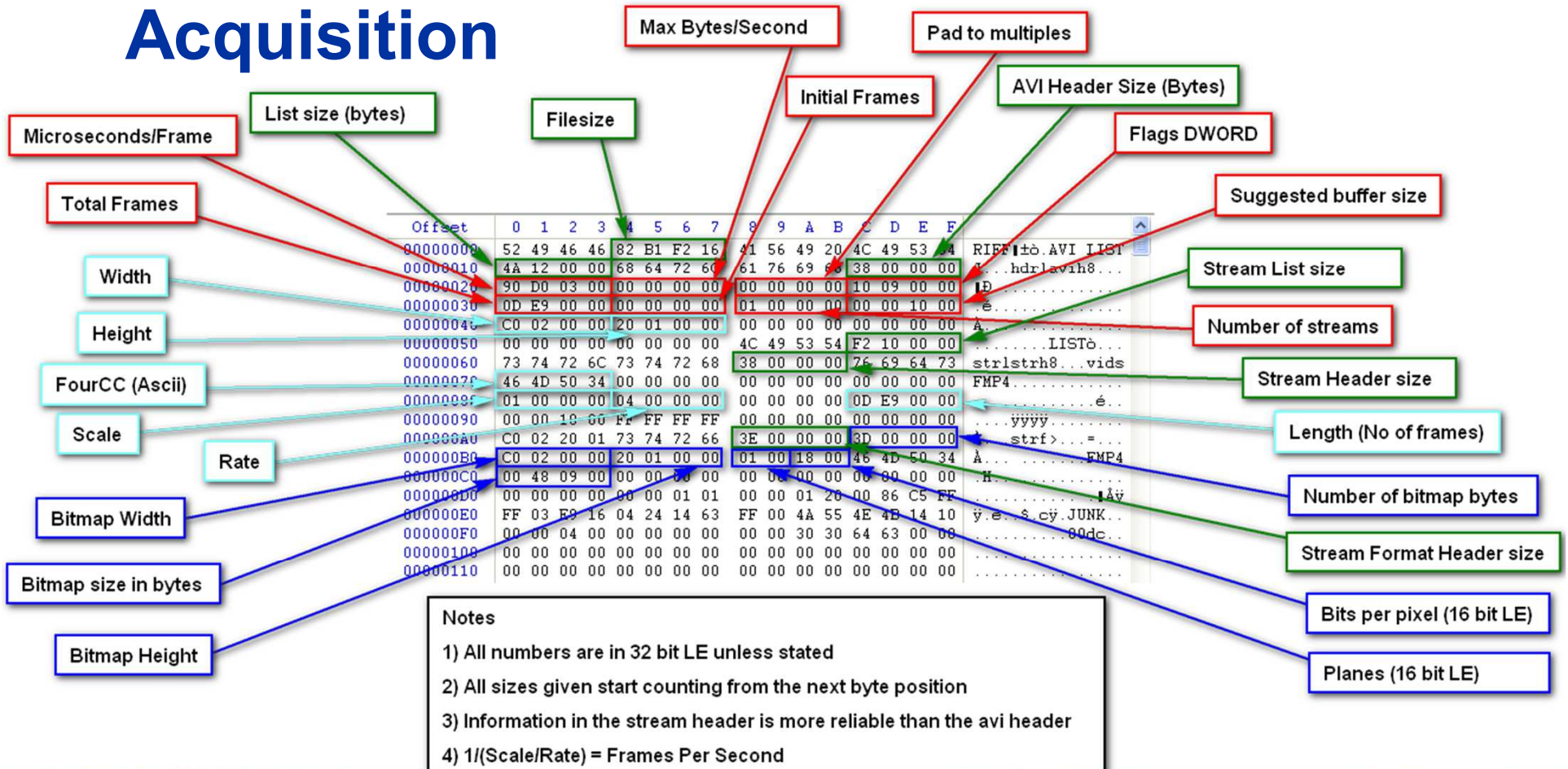
# Acquisition

Offset	0	1	2	3	4	5	6	7	
00000000	00	00	00	B9	73	74	73	64	'stsd
00000008	00	00	00	00	00	00	00	01	
00000010	00	00	00	A9	6D	70	34	76	@mp4v
00000018	00	00	00	00	00	00	00	01	
00000020	00	00	00	00	00	00	00	00	
00000028	00	00	00	00	00	00	00	00	
00000030	01	60	01	20	00	48	00	00	H
00000038	00	48	00	00	00	00	00	00	H
00000040	00	01	00	00	00	00	00	00	
00000048	00	00	00	00	00	00	00	00	
00000050	00	00	00	00	00	00	00	00	
00000058	00	00	00	00	00	00	00	00	
00000060	00	00	00	18	FF	FF	00	00	yy
00000068	00	43	65	73	64	73	00	00	Cesds
00000070	00	00	03	80	80	80	32	00	!!!2
00000078	01	00	04	80	80	80	24	20	!!!\$
00000080	11	00	00	00	00	09	23	CA	#E
00000088	00	09	23	CA	05	80	80	80	#E !!!
00000090	12	00	00	01	00	00	00	01	
00000098	20	00	88	40	19	28	58	21	!@ (X!
00000A00	20	A3	1F	06	80	80	80	01	£ !!!
00000A80	02	00	00	00	10	70	61	73	pas

Annotations:

- Size of atom:** Points to the first byte (00) at offset 00000000.
- Width (16 bit BE):** Points to the first two bytes (01 60) at offset 00000030.
- Height (16 bit BE):** Points to the next two bytes (01 20) at offset 00000032.
- moov>trak>mdia>minf>stbl>stsd Sample Description:** Points to the 'stsd' field at offset 00000000.
- Codec information (e.g. mpeg-4 visual):** Points to the '@mp4v' field at offset 00000010.
- moov>trak>mdia>minf>stbl>stsd>esds Elementary stream sample description:** Points to the 'yy Cesds' field at offset 00000060.
- VOL header from mpeg-4 visual bitstream:** Points to the '!@ (X!' field at offset 00000098.

# Acquisition



POLICE

Gareth.Harbord@met.police.uk





# Acquisition

- Find the footage



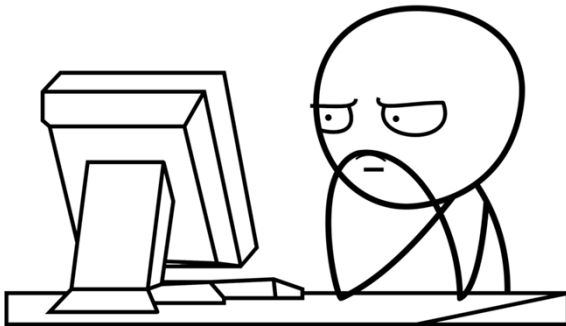
**METROPOLITAN  
POLICE**

Gareth.Harbord@met.police.uk



# Acquisition

- Write some code



```
1 reference
public void ProcessExport()
{
    int counter = 0;

    using (FileStream inFs = new FileStream(fileNames.InputData, FileMode.Open, FileAccess.Read))
    {
        foreach (TimeRange timeRange in timeRanges)
        {
            string fileOut = Path.Combine(fileNames.OutputFolder, timeRange.GetFileName());
            using (FileStream outFs = new FileStream(fileOut, FileMode.CreateNew, FileAccess.Write))
            {
                if (counter == timeRanges.Count-1)
                {
                    int bufferSize = (int)(inFs.Length - timeRange.InOffset);
                    inFs.Seek(timeRange.InOffset, SeekOrigin.Begin);
                    byte[] buffer = new byte[bufferSize];
                    inFs.Read(buffer, offset:0, count:bufferSize);
                    outFs.Write(buffer, offset:0, count:bufferSize);
                }
                else
                {
                    int bufferSize = (int)(timeRanges[counter + 1].InOffset - timeRange.InOffset);
                    inFs.Seek(timeRange.InOffset, SeekOrigin.Begin);
                    byte[] buffer = new byte[bufferSize];
                    inFs.Read(buffer, offset:0, count:bufferSize);
                    outFs.Write(buffer, offset:0, count:bufferSize);
                }
            }
            counter++;
        }
    }
}
```

# Ingest



**METROPOLITAN  
POLICE**

Gareth.Harbord@met.police.uk



# Screen Capture



Gareth.Harbord@met.police.uk



# Screen Capture

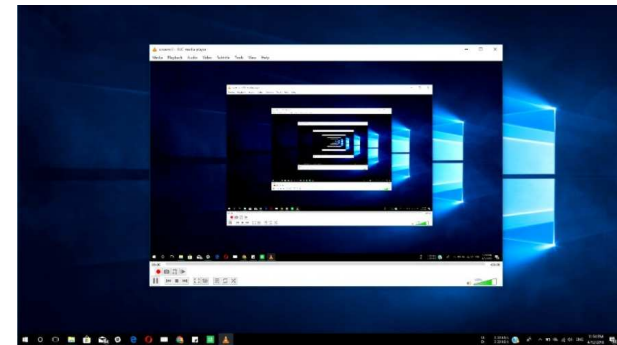
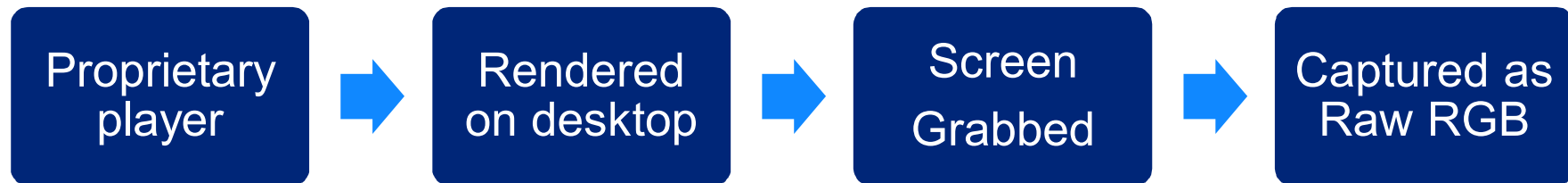
- CCTV exports in proprietary containers.
- Legacy systems used more exotic codecs e.g. ADV601, GEOX, SMAC-M...
- Difficult to transcode.



Gareth.Harbord@met.police.uk

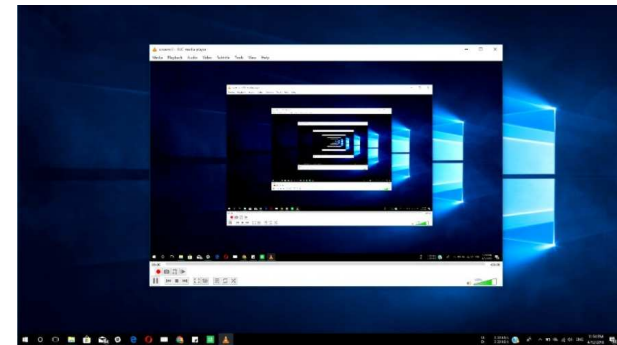


# Screen Capture



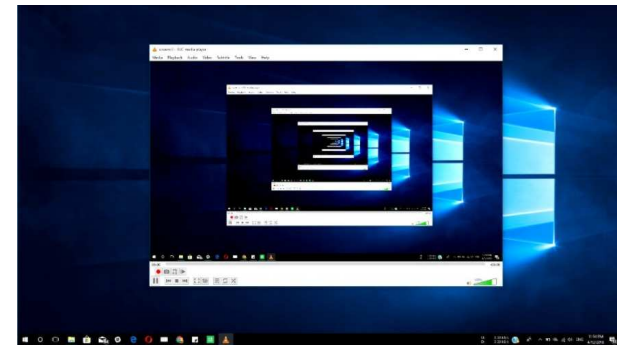
## Screen Capture – Pros

- Simple process
- Limited technical knowledge required
- Native player may display time and date as an On Screen Display (OSD) overlay



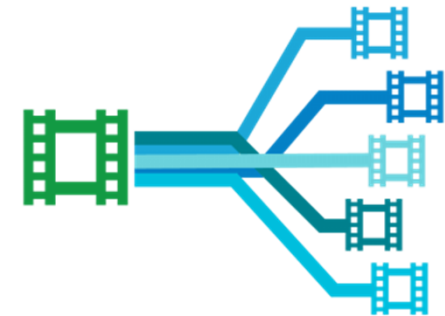
## Screen Capture – Cons

- Unavoidable colour space conversion i.e. YUV420 -> RGB24
- Dropped frames/Scaling issues
- Endless executables
- Real-time capture
- Requires transcoding to conform frame-rates/reduce data size





# Transcoding



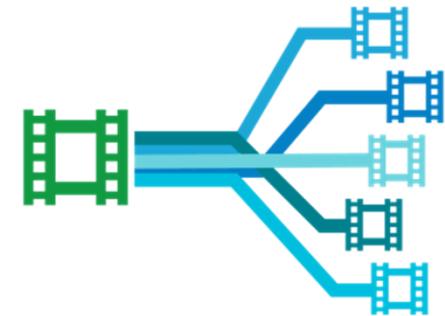
**METROPOLITAN  
POLICE**

Gareth.Harbord@met.police.uk

NEW  
SCOTLAND  
YARD

## Transcoding - Pros

- Maintain colour space/less vulnerable to clipping
- Less likely to crop image edges
- Better with interlaced sources
- Faster than real-time
- No executable



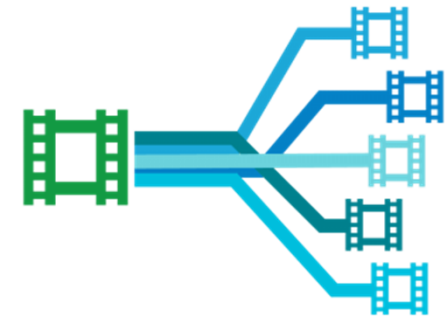
**METROPOLITAN  
POLICE**

Gareth.Harbord@met.police.uk

NEW  
SCOTLAND  
YARD

# Transcoding - Cons

- Not all formats compatible
- OSD overlays cannot be captured
- Unpredictable behaviour
- Timing can be lost



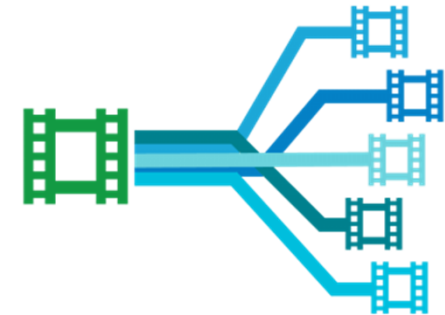
**METROPOLITAN  
POLICE**

Gareth.Harbord@met.police.uk

NEW  
SCOTLAND  
YARD

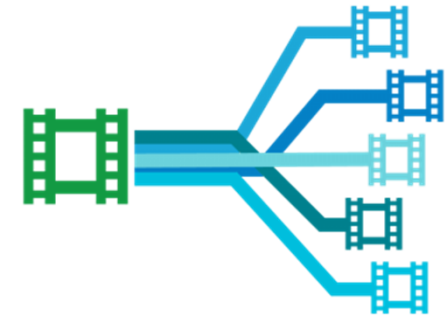
# Rewrapping

- Ideal for enhancement
- Sometimes pre-transcode
- Trial and error involved
- Timecode repair



# Ingest

- Currently using 8-bit libx264 lossless as intermediate format
- Video conformed to 30fps
- Scaled to 1920\*1080
- Mastering to DNX MOV
- Distributing as MP4 via ffmpeg



**METROPOLITAN  
POLICE**

Gareth.Harbord@met.police.uk

NEW  
SCOTLAND  
YARD

# Presentation

- Court replay systems problematic
- Wireless streaming degrades replay
- Presentation team educate officers
- In-house presentation software



# Questions?



**METROPOLITAN  
POLICE**

Gareth.Harbord@met.police.uk



# Editing



**METROPOLITAN  
POLICE**

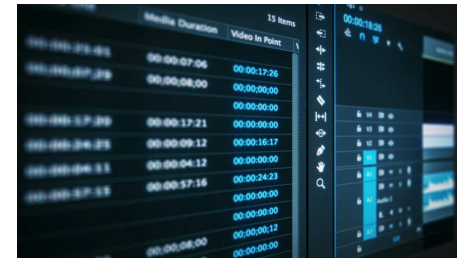
Gareth.Harbord@met.police.uk





# Editing

- May edit clips from CIF to 4K on same timeline.
- Using a 1920\*1080 timeline
- Video ordered chronologically
- Highlighting sometimes required
- Avoid adding titles



# Editing

- Adjustment
  - Light levels/Gamma



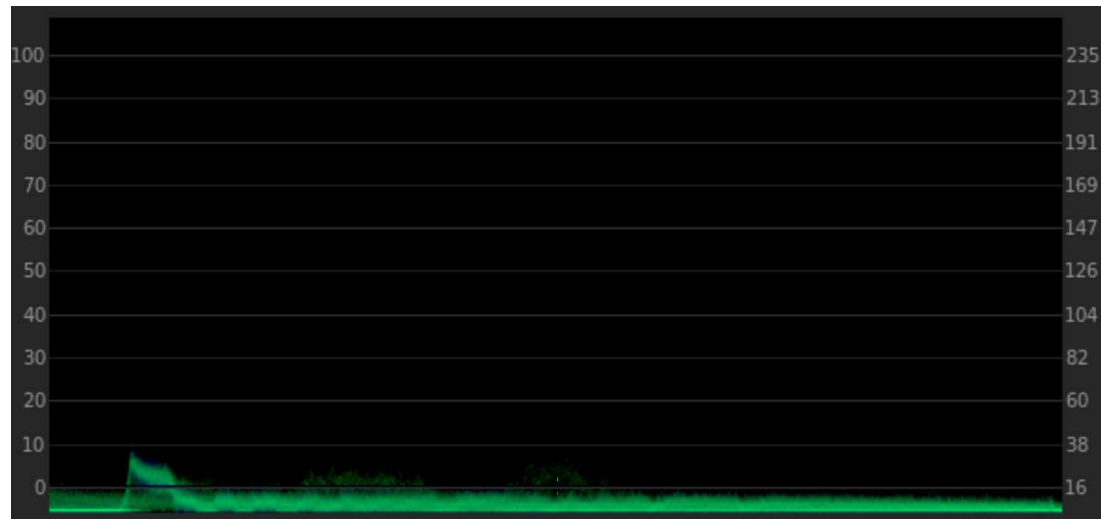
**METROPOLITAN  
POLICE**

Gareth.Harbord@met.police.uk



# Editing

- Adjustment
  - Light levels/Gamma – Use a waveform monitor



**METROPOLITAN  
POLICE**

Gareth.Harbord@met.police.uk



# Editing

- Adjustment
  - Noise Reduction

Original



Noisy image



Denoised image



**METROPOLITAN  
POLICE**

Gareth.Harbord@met.police.uk



# Editing

- Adjustment
  - Stabilization



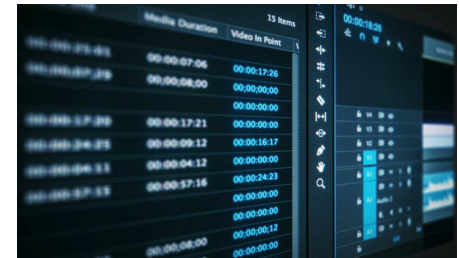
**METROPOLITAN  
POLICE**

Gareth.Harbord@met.police.uk



# Editing

- Timeline mastered as DNX MOV then produced as H.264 MP4
- Chapter markers useful
- Menu systems all but abandoned



# Enhancement



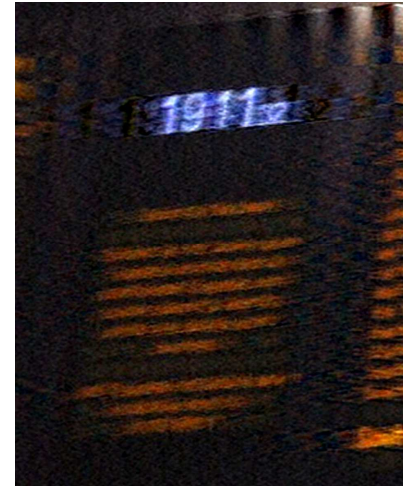
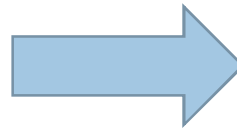
**METROPOLITAN  
POLICE**

Gareth.Harbord@met.police.uk



# Enhancement

- Blind Deconvolution



**METROPOLITAN  
POLICE**

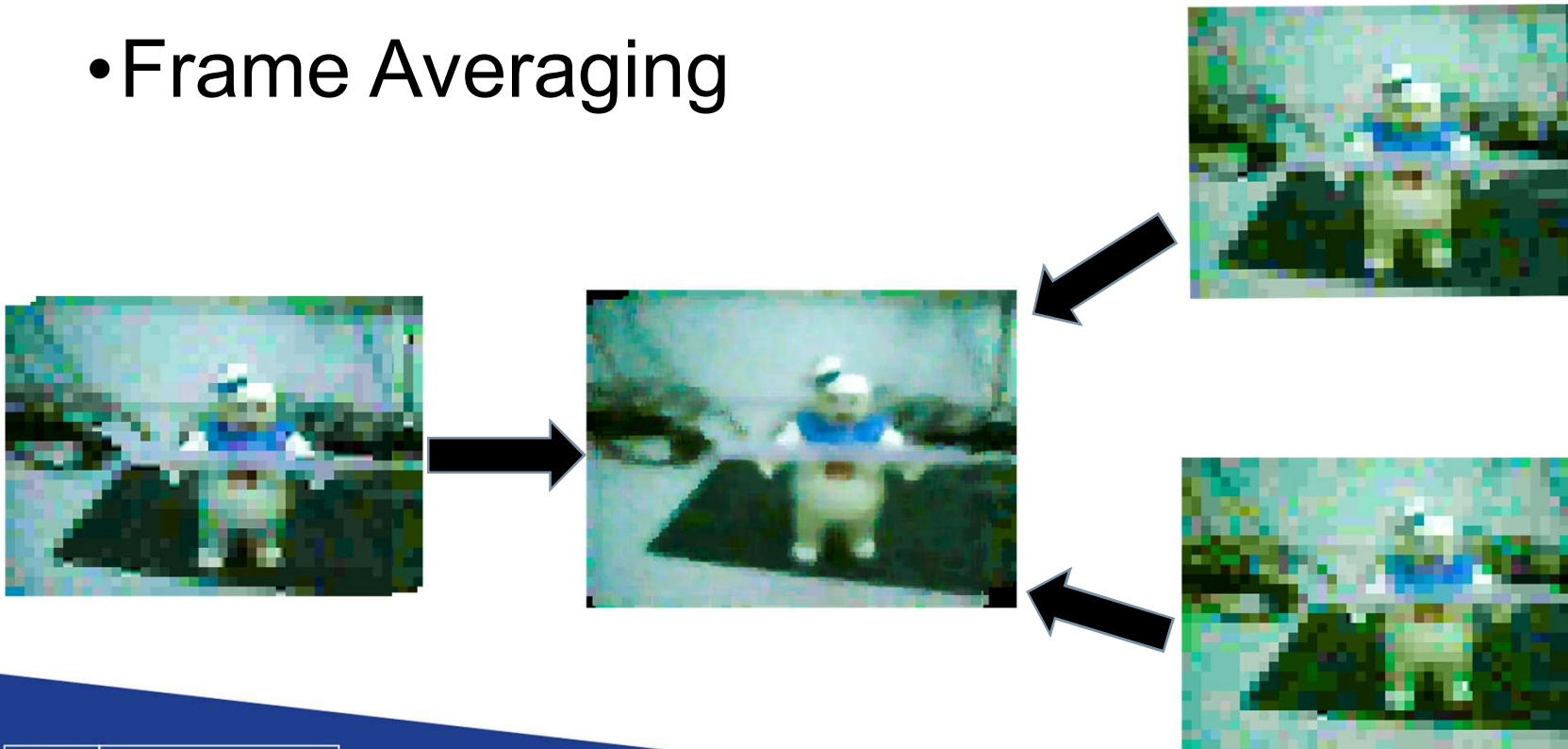
Gareth.Harbord@met.police.uk





# Enhancement

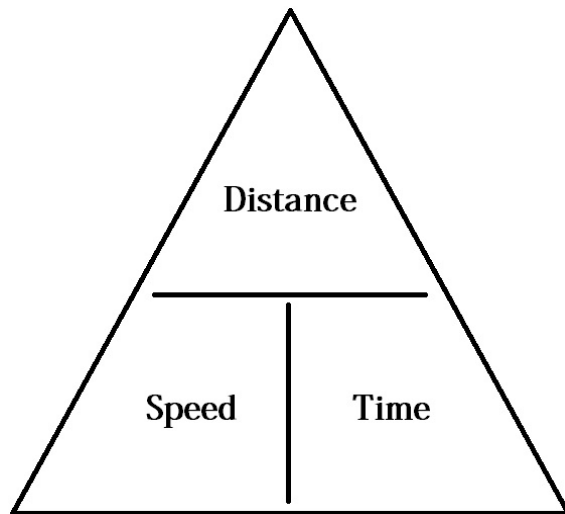
- Frame Averaging





# Enhancement

- Speed analysis



**METROPOLITAN  
POLICE**

Gareth.Harbord@met.police.uk



# Questions?



**METROPOLITAN  
POLICE**

Gareth.Harbord@met.police.uk

