Management Analytics

A Tale of Two Traces
Archives, Diplomatics, and Digital Forensics

2015-01-26
Orlando, FL

Dr. Fred Cohen

Management Analytics

Outline

- Background and problems
  - Selling my house in Livermore
  - Causality, Diplomatics, Public records, and selling my house...
  - A business partnership ends
  - Digital records, Digital diplomatics, and the end of a partnership
  - Forensic science, and digital forensics, and the rest of this paper
- Digital diplomatics vs. Forensics vs. Digital forensics and cases
- Resolution
- Implications and a path forward
- Discussion

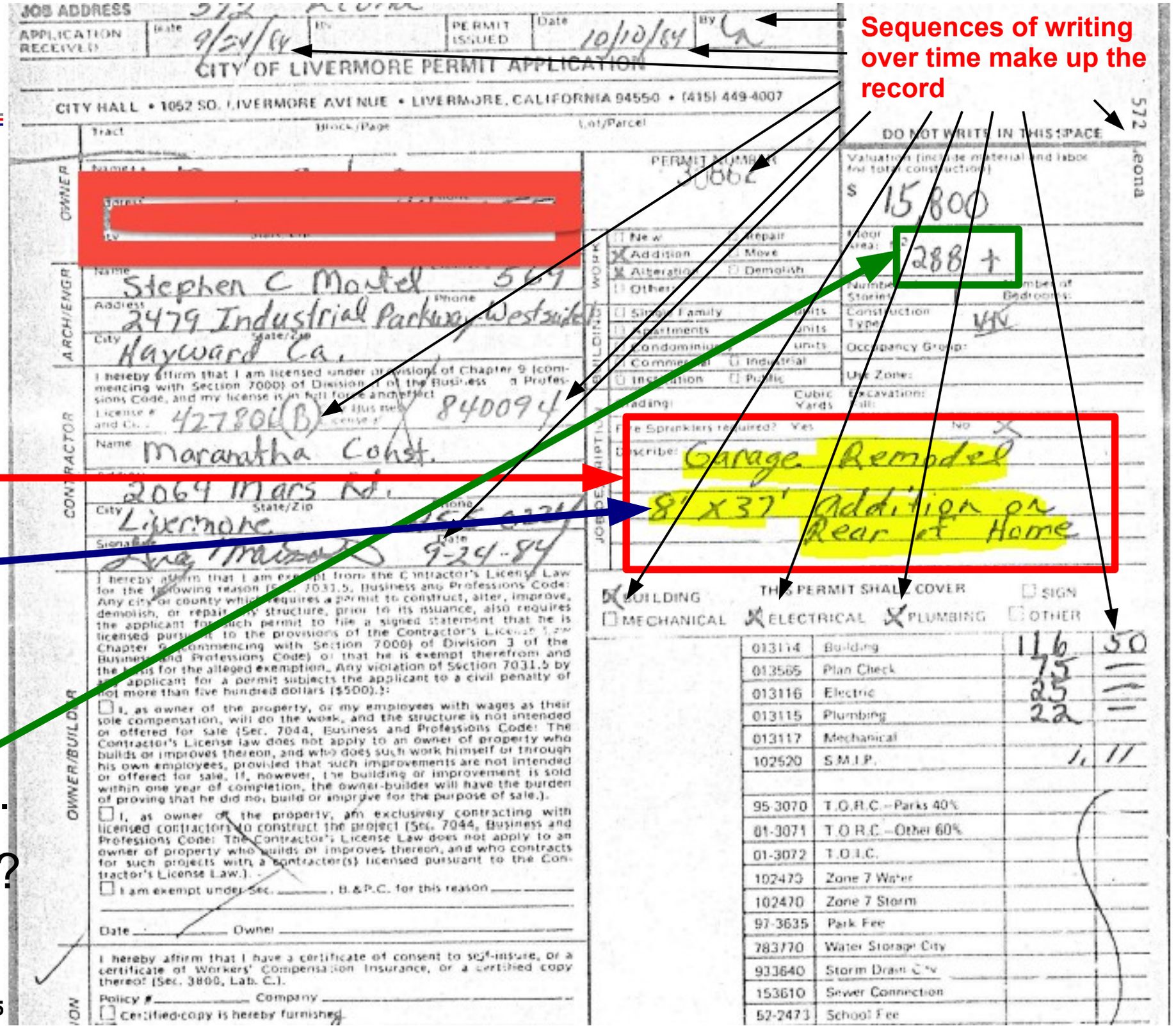
Management Analytics

I was trying to sell my house in Livermore

- Lots of paperwork and formal interaction with government
  - The whole history of the property and structures
  - All of the permitted activities performed
  - All of the tax history
  - Untold different versions of paperwork over 50+ years
- Come a week before closing...
  - The square footage of the house came into dispute
    - Taxes are based on square footage and sale value
    - The buyer thought we were lying about the square footage
  - They backed it up with the public records at the city
  - They wanted to pay less or not close the deal
- Note the form of the public records

Management Analytics

- The disputed garage addition
- 8*37=296
- !=288 sq. ft. floor space?



Management Analytics

The nature of such records

- Diplomatic analysis of such records is fairly interesting (to me)
  - Sequences of markings and annotations are made over time
  - Each of a set of different parties must make annotations
  - Requests, signatories, various parties, approvals, etc.
  - Redundancy within the records (e.g., sq. ft. and dimensions)
  - Seals and stamps (e.g., permit number when issued stamped)
- This record is part of the fonds of the public records
  - The fonds of the various parties include many other records
  - Similar records have similar appearances and markings
  - Signatures of the same party can be compared
  - The permit number and date are sequential (missing/added?)
  - Presumed reliable and accurate for legal purposes

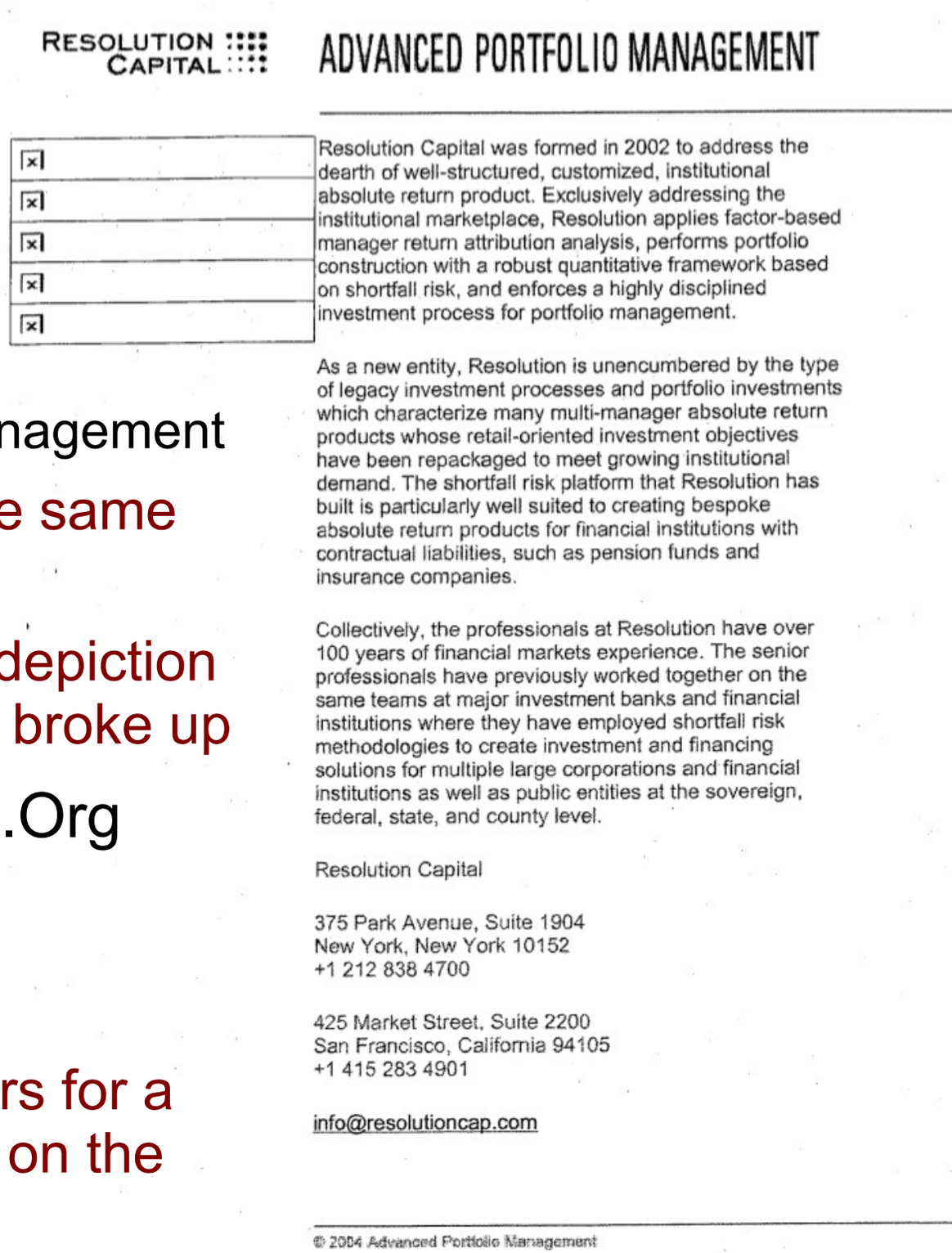
Management Analytics

Partners broke up their investment firm

- After the firm broke up, each went their separate ways
  - Partner 1 retained ownership of their domain name
  - Partner 1 started a new investment firm using that domain
  - Partner 2 went a different direction
- A few years later, Partner 2 was unhappy
  - Decided to sue Partner 1 for whatever set of reasons
  - In seeking evidence, Partner 2 found something
    - Evidence that Partner 1 was already starting the new firm before the old firm broke up!
  - This would prove Partner 1 did not fulfill fiduciary responsibilities
    - Loyalty to the partnership
  - And perhaps that Partner 1 used Partner 2 for unlawful gain
    - A fraud of oe form or another

The traces

- Looks bad for Partner 1
  - Two companies
    - Resolution Capital
    - Advanced Portfolio Management
  - They appear together at the same time on the same Web site
  - The date identified for this depiction was before the partnership broke up
- The source of the data: Archive.Org
  - The Internet Archive
  - Their "Wayback Machine"
  - Often used by LE and others for a historical view of what was on the Web over time



RESOLUTION CAPITAL

ADVANCED PORTFOLIO MANAGEMENT

Resolution Capital was formed in 2002 to address the dearth of well-structured, customized, institutional absolute return product. Exclusively addressing the institutional marketplace, Resolution applies factor-based manager return attribution analysis, performs portfolio construction with a robust quantitative framework based on shortfall risk, and enforces a highly disciplined investment process for portfolio management.

As a new entity, Resolution is unencumbered by the type of legacy investment processes and portfolio investments which characterize many multi-manager absolute return products whose retail-oriented investment objectives have been repackaged to meet growing institutional demand. The shortfall risk platform that Resolution has built is particularly well suited to creating bespoke absolute return products for financial institutions with contractual liabilities, such as pension funds and insurance companies.

Collectively, the professionals at Resolution have over 100 years of financial markets experience. The senior professionals have previously worked together on the same teams at major investment banks and financial institutions where they have employed shortfall risk methodologies to create investment and financing solutions for multiple large corporations and financial institutions as well as public entities at the sovereign, federal, state, and county level.

Resolution Capital

375 Park Avenue, Suite 1904
New York, New York 10152
+1 212 838 4700

425 Market Street, Suite 2200
San Francisco, California 94105
+1 415 283 4901

info@resolutioncap.com

© 2004 Advanced Portfolio Management

Management Analytics

The nature of such traces

- Diplomatic analysis of such traces is not yet clear
  - Provenance is not clear and not provided
  - It is not kept with data related to the fonds
  - It is presented as a composition without obvious markings
  - Seals, signatures, underlying process, are not well defined
  - The process by which the fonds come to be changes
    - Without notice, without records of the change, etc.
- This depiction is the result of a private collection projected
  - No transparency as to process → Cannot tell how it work(ed/s)
  - Projected depiction is different in different browsers / screens
  - Depiction changes with browser settings and other things
  - Depiction may change over time based on underlying operations

Management Analytics

You can read the paper...

- I summarize briefly
  - Forensic science
    - Well developed over a long time and still dramatically changing
    - But it does allow examination of physical records
    - Especially good from archives and public records
  - Digital forensics
    - Very new, very limited, and dramatically changing
    - It allows various sorts of examination of digital traces
    - Lacks formal diplomatic analysis and consistent everything
    - Especially bad for authenticity and reliability of records
  - The rest of the paper
    - A fascinating tale of deception and love, …
    - Not really - so I'll just get to the interesting part

Management Analytics

Outline

- Background and problems
- Digital diplomatics vs. Forensics vs. Digital forensics and cases
  - There are lots of things going wrong today
    - Here are some examples...
- Resolution
- Implications and a path forward
- Discussion

Management Analytics

Some (other) things that go (went) wrong

- Docusign
  - A service for doing signatures of documents over the Internet
  - A minor problem in that what you sign != what they get
    - Same deal - I got a document with the wrong box checked
      - Not a trivial check mark - something about liability and ownership
    - I called the realtor - resend?
      - The realtor checked the document to be signed
      - The document she saw had the other check box checked!
    - She said - sign it, she will verify the result before sending it on
      - The document I 'signed' was not the document that resulted
      - The end result was actually right (but not what I signed)
- All sorts of "cheat and fix" things
  - Nearly every digital act ended up with a cheat and fix like that
  - Thankfully, the final actual documents are still on paper
    - Physical signatures attested by human on site

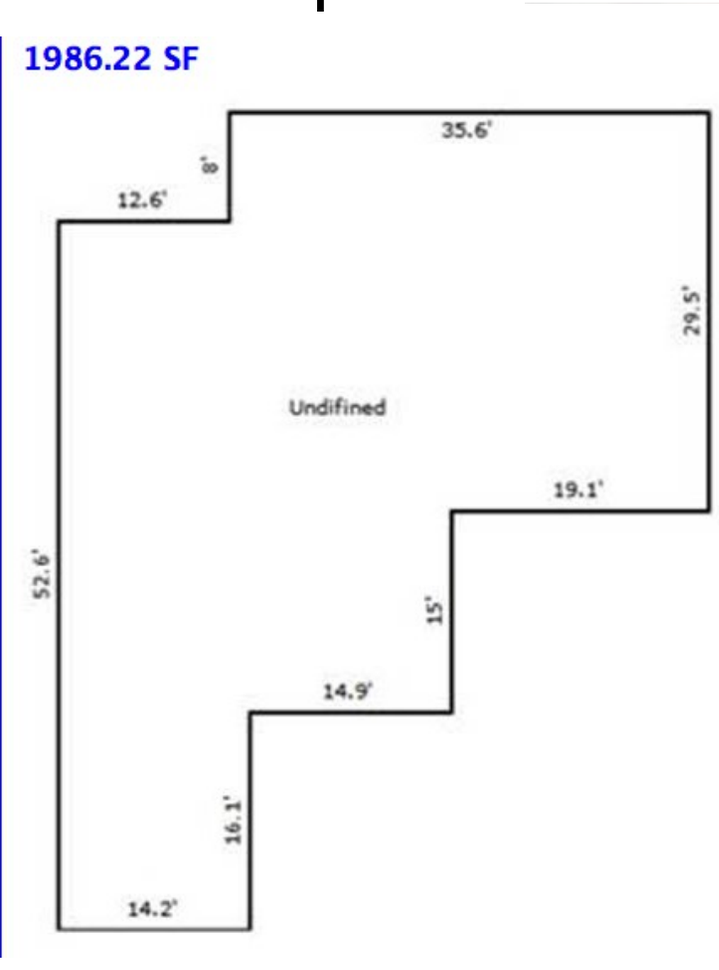
Management Analytics

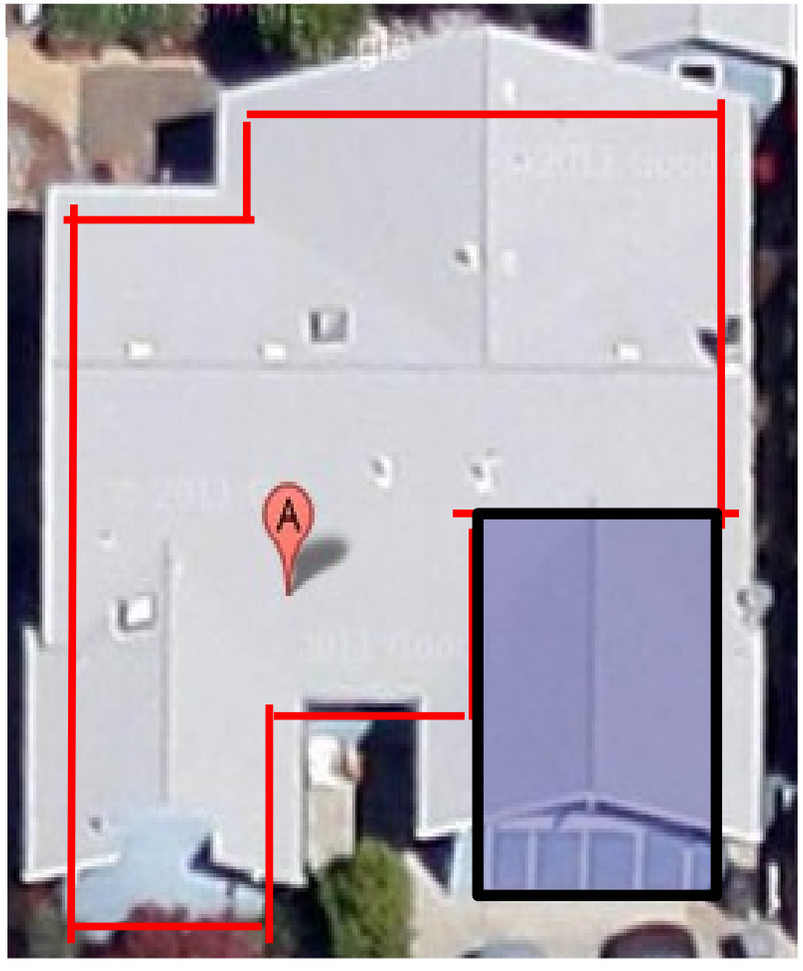
Outline

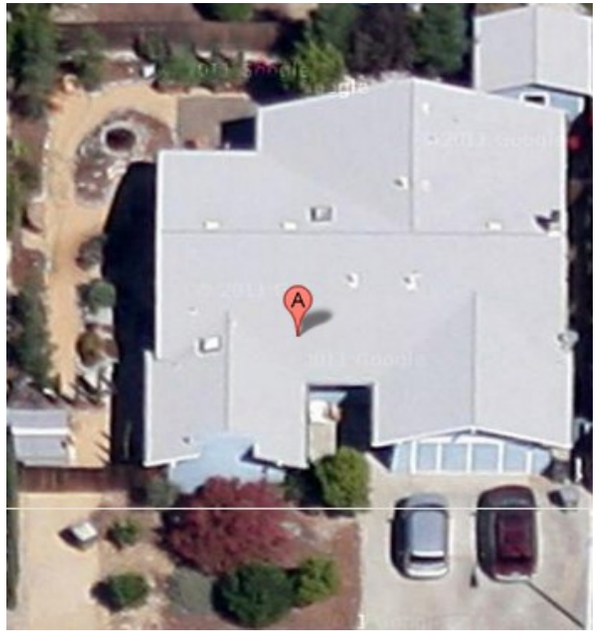
- Background and problems
- Digital diplomatics vs. Forensics vs. Digital forensics and cases
- Resolution
  - Case 1 - paper records, redundancy, and resolution
  - Case 2 - digital records, redundancy, and resolution, … however
- Implications and a path forward
- Discussion

Case 1 - An apparent inconsistency

- Building inspector produces 1986.22 sq. ft. analysis based on limited public record search and measurements







Google Earth View of the property

- It appears that the reality and the theory don't fully align!
  - **Missing ~19.2' x 15' = 288 sq. ft. section**

RESIDENTIAL BUILDING SHEET

ADDRESS [redacted]

PARCEL 99-320-79 SHEET 1 OF 21 SHEETS

DESCRIPTION OF BUILDING

CLASS & SHAPE: D-6-A
ARCHITECTURE: 1 Stories
USE TYPE: Single, Conv., Double, Duplex, Apartment, Flat, Court, Motel, Units
CONSTRUCTION: Light, Sub-standard, Standard, Above-Standard, Special
FOUNDATION: Concrete, Reinforced, Brick, Wood, Piers, Light, Heavy
STRUCTURAL: Frame 2"x4"-16", Line Wire, Sheathing, Conc. Block, B & B, T & G, Brick, Adobe, Flr. Construction, 1st, 2nd, Conc. Slab, Sub Flr., Bsm't Flr., Insulation
EXTERIOR: Stucco on Wi., Rustic, W-Shingle, Asb. Shingle, Shake, B & B, Brick, T & G, Stone, Trim
WINDOWS: D.H., Wood, Csm't, Alum., Sliding, Steel, Screens
ROOF: Flat, Pitch, Gable, Hip, Shed, Cut Up, Dormers, Boxed Eaves, Gutters, Tl, Tl Trim, Shake, Wood Shi., Compo. Shi., Tar & Gravel
LIGHTING / WIRING: K.T., Conduit, B.X., Cable, 220
FIXTURES: Few, Cheap, Ave., Medium, M'ny, Special
PLUMBING: Poor, Good, Fixtures, Water Heater, Gas, Elect.
AIR CONDITION: Heating, Cooling, Forced, Clean'g, Gravity, Humid, Central, Wall Unit, Floor Unit, Single, Dbl., Radiant, Perimeter, Steam, H. Wtr, Thermostat, M.B.T.U., F.P., B.B.Q.

ROOM AND FINISH DETAIL

ROOMS	FLOORS B	1	2	3	Typ	FLOOR FINISH Material	Grade	TRIM	INTERIOR FINISH Walls	Ceilings
All						[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
FAL-B						TI			UNF	
Ent. Hall						[illegible]				
Living										
Dining										
[illegible]						[illegible]				
Bed										
Bed										
AD I-A						WW CPT			SR+TEX	AC OUS
AD I						7'UN			PA/SRTX	ACOUS
[illegible]						[illegible]		[illegible]	[illegible]	[illegible]
Kitchen						[illegible]			[illegible]	[illegible]

Drain Bd. Material [illegible] Lgth. 20 Ft. Splash [illegible]

CONSTRUCTION RECORD

Permit No.	For	Amount	Date	EFFEC. YEAR	APPR. YEAR	Age	Remain'g Life	Table	%	Cond.	Arch Attr.	Func. Plan	Con-form	Storage Space Cupbd	Closet	Work-manship
3453	NC	18728	7-66	1968	1968	0	60	R60	100	A	A	G	G	A	A	A
12710	ADD	1300	8-72													
6457	[illegible]	2300	[illegible]													
30862	ADD	15800	10-84													
A5W39	RMDL	22,000	11-8-85													

BATH DETAIL

Fl.	No.	Floors	Walls	Wc	La	Tub	Type	Grade	St	OT	SD	Finish
1	1	[illegible]	[illegible]	1	1	1	[illegible]	[illegible]				[illegible]
1	3/4	[illegible]	[illegible]	1	1		[illegible]	[illegible]	1		1	[illegible]
1	3/4	VIN	SR+EN	1	1	1	MOD	STD	1			FYBRE

SPECIAL FEATURES: Book Cases, Vanity, S/Glass Door, Disposal, Hood & Fan
EXTRA EQUIPMENT: Range/Oven, Dishwasher, Inter Comm

COMPUTATION

5/18/68 - MG

Appraiser & Date Unit	Area	Unit Cost	Cost	VARGAS 7-24-76 Unit Cost	Cost	SOBASE 8-05-85 Unit Cost	Cost
RES.	1704	8.55	14569				
LND	171456	.50	1271				
AC-P			600				
FP			420				
1-[illegible]			500				
[illegible]	420	.40	182				
FENCE	30	2.00	60				
WALL	15	3.00	45				
[illegible] 2/3	20	.70	144			RMKS	- 48
					3.30		
ADI	288					56.81	+ 16361
AC-B	288					1.30	+ 374
FA-1-B	285					Remmekes	+ 4008
AL-C	285						+ 345
TOTAL			17,794		21094	NET CHG. =	
NORMAL % GOOD			100		100	+ 21040	
R.C.L.N.D.			17,794		21094		

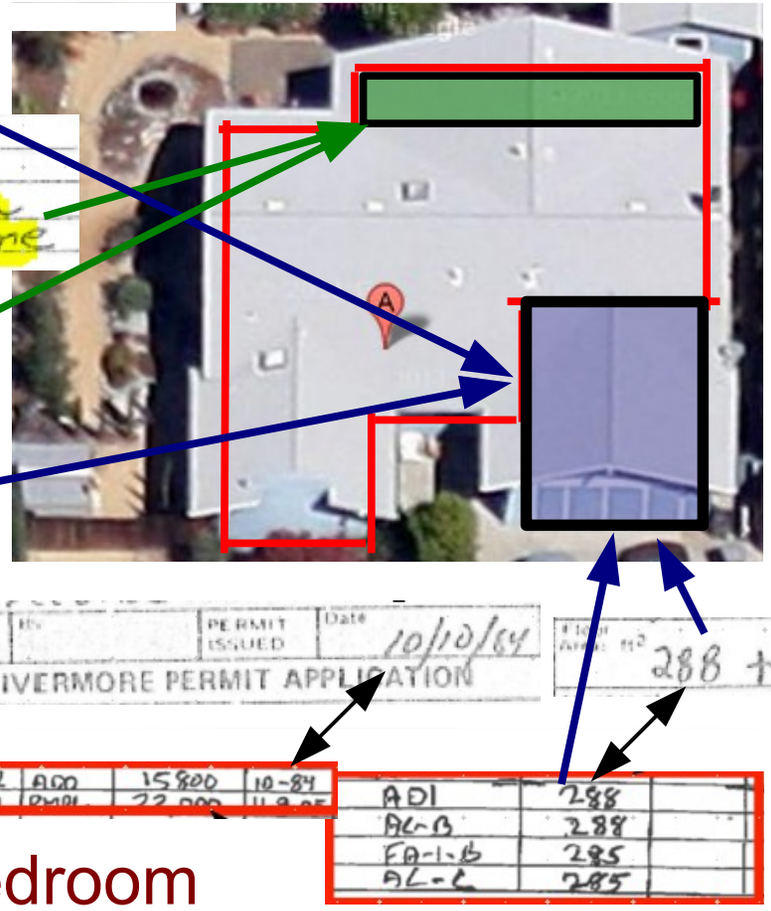
The tax records from the county show the addition of 288 sq.ft. as of 10-84 - the tax records agree with the permit records and not the building inspector. Tax is based on tax records

Form 111-30-87 Rev. 1966

06 JUL [illegible]   AUG 4 1976

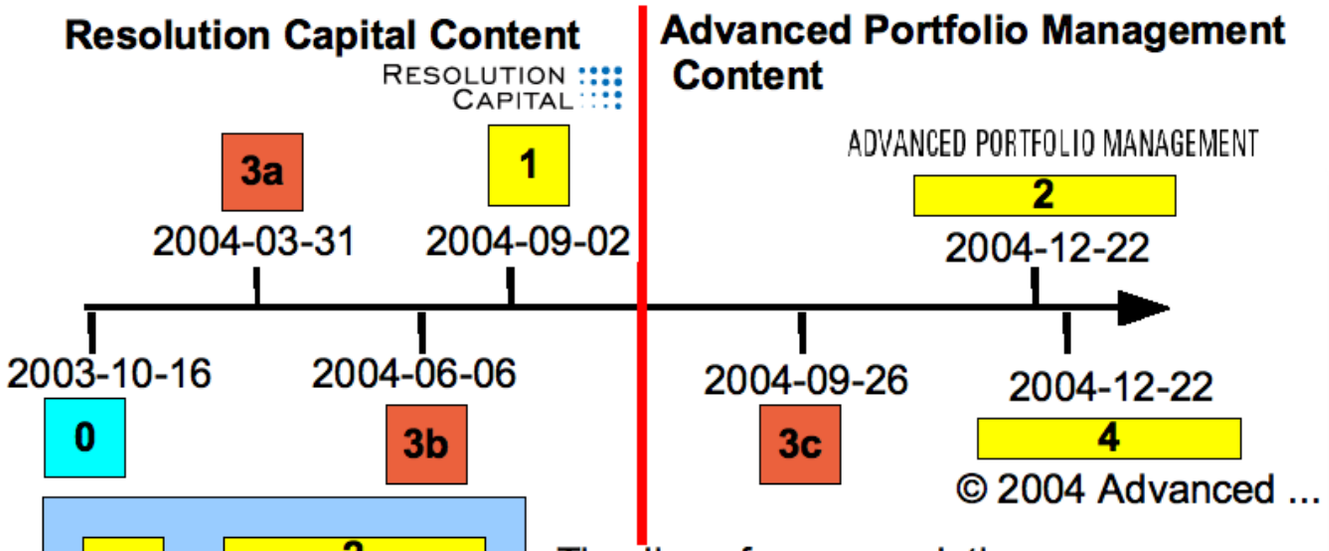
Some calculations and redundant records

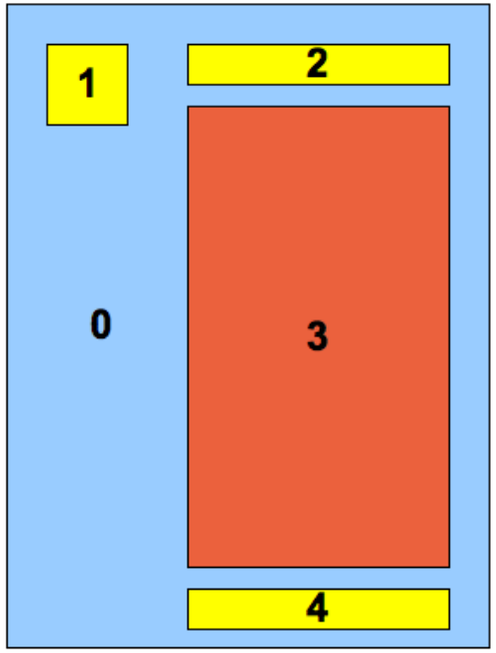
- What is going on?
  - In 1984, two things happened
  - A garage remodel
  - An addition on the rear of home
- An 8'x37' addition (8*37= 296 sq. ft.)
- Garage ~19.2' x 15' = 288 sq. ft.
- Net house size is about 'living space'
  - The nature of the garage changed
  - No longer a garage - laundry room / bedroom
  - The rear addition was pre-calculated into the pre +288 size
- Note the redundant records and how things match up
  - Redundant authentic records are how these disputes are settled



Case 2 - Resolution

- Different areas of the screen fused from different times led to the inaccurate depiction on the WayBack Machine. It never existed on the real Web site as depicted in WayBack

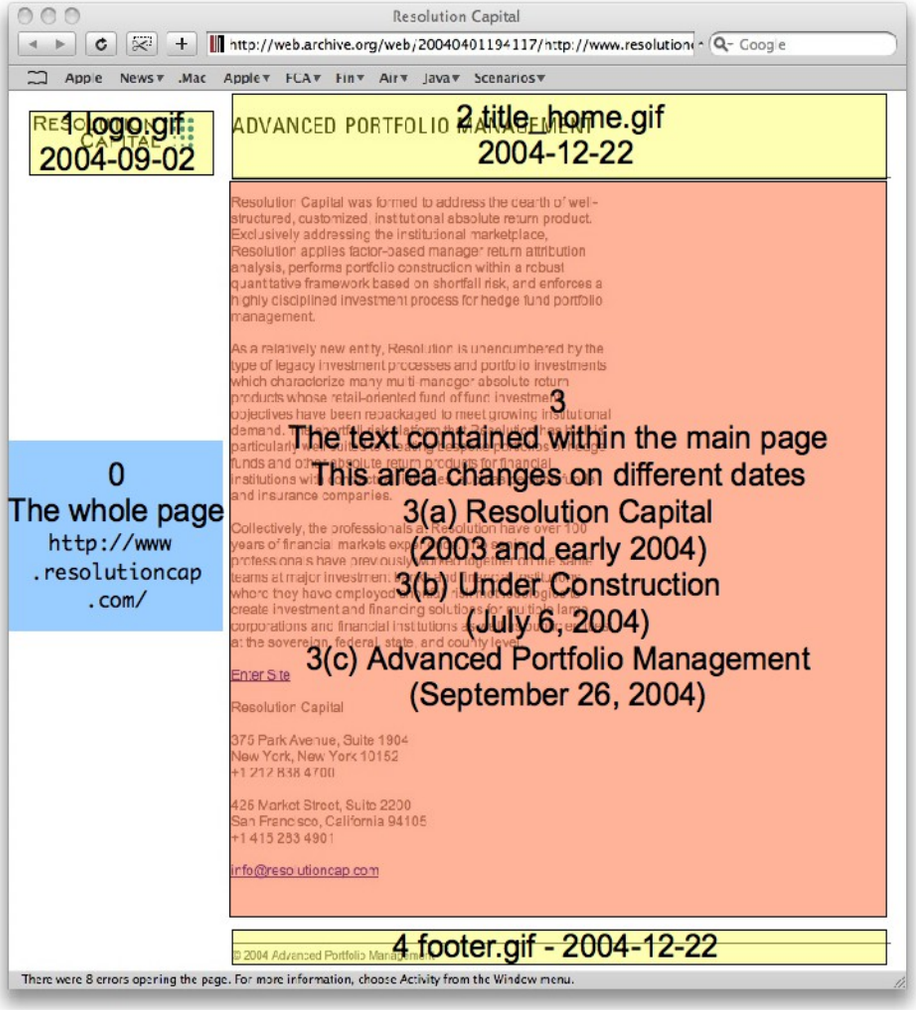




Timeline of www.resolutioncap.com based on the time and date information from the WayBack Machine – not to scale

- 2004-09-02: the last content containing "Resolution Capital" was gathered
- 2004-09-26: the first content containing "Advanced Portfolio Management" was gathered

Even though the depiction seen in a Web browser from the WayBack Machine makes it seem like these two were together the evidence does not support it.



Management Analytics

The WayBack Machine...

- At the time at issue...
  - Example from the WayBack Machine
  - Shows graphics from different dates combined as depictions that can not reflect reality at any given time.
  - This particular example will not work today!
  - We need to apply the technology of the day.
  - Which is no longer available!!
- Timely reconstruction was necessary to resolution!

The Wayback machine is not a reliable tool for digital forensics.

The proof:
Turn off Javascript
Go to the wayback machine (www.archive.org)
Search for http://all.net/
Click on the first entry – the one from 1997

You will see this ".gif" file on part of the screen...

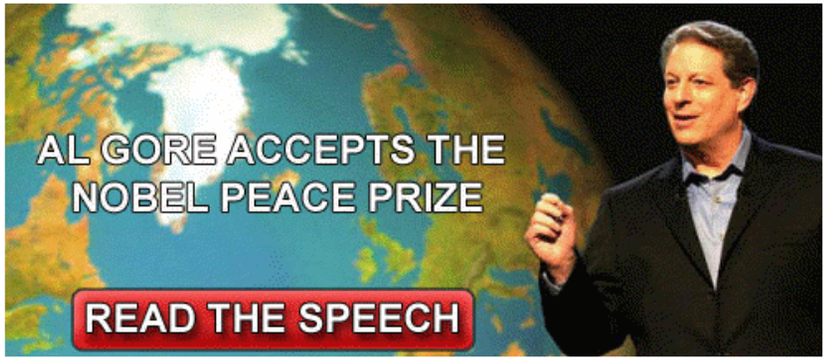
The US was attacked on 9/11/2001 by radical islamist terrorists.
There were no weapons of mass destruction found in Iraq.
GW Bush was re-elected
Al Gore won a Nobel prize and an oscar for global warming worl
Put the details of your case here for proof to the judge and jury..

Either I am a time traveller
OR I am the best guesser of all time.
OR the Wayback machine is not always a reliable tool for digital forensics.

And I can prove it in court.

For more details, go to http://all.net and get in touch with me.

FC



Management Analytics

A major problem with Case 2

- If I hadn't reconstructed at that time...
  - The reconstruction would not have worked
  - The depicted trace would have not been demonstrably false
  - The case may have been resolved differently
    - It certainly would have cost a lot more for all parties
- The WayBack machine is one of the better unreliable sources
  - Still unreliable from a standpoint of what may get depicted
  - But at least there are date and time stamps of collection
    - Even though they show the same "gif" it may also change
    - We did a demonstration with the naval observatory clock...
  - Not as transparent as public archives
    - But more so than most Internet sites

Management Analytics

Outline

- Background and problems
- Digital diplomatics vs. Forensics vs. Digital forensics and cases
- Resolution
- Implications and a path forward
  - There lies the rub
- Discussion

Management Analytics

There are way too many problems with this...

- Unknown mechanisms (lack of transparency)
- Performing unknown or incorrectly documented acts (collection)
- Producing false depictions / for legal signature & use
- Depicted using a wide range of mechanisms (viewers / browsers)
- Saved by some of those entities (repositories of all sorts)
- Without documented or controlled fonds or markings
- Without apparent redundancy / separation of duties / etc.
- Presented as evidence in legal settings
- Without adequate (or much of any) provenance
- Lacking reliability or authenticity and stored in unreliable systems
- And they look really good and seem compelling!

Management Analytics

What do we do about it?

- Assume tasks are performed by qualified individual(s)
  - And make sure to produce enough of them and require their use
- Track who did what when at a detailed level and retain as records
- Documentary forms should be identified, defined, kept, and used
  - Including all relevant forms used and likely to be used
    - In imitative copy form that can be reliably viewed locally as identical to the original, entirely contained in the stored form
- Things to retain:
  - URLs, sources for Web pages or other content retrieved
    - Stored in an imitative copy form as for documentary forms above
  - Copies of whatever is collected in computer-usable form
    - In addition to the imitative copy, actual content

Management Analytics

What to do about it

- Things to retain:
  - Fonds details including all relevant versions and documentation
  - Elements of the archival bond
    - Storage formats like YYYY-MM-DD-vvv …
    - Metadata files stored locally and independently in catalog
    - Following existing standards (COP table)
  - Test procedures, results, tools, calibration, etc.
  - Transparency information and relevant personnel records, etc.
  - Supporting documents for names protocols (e.g., RFC791, etc.)
  - … (other things listed in the paper)
- Lacking existing consensus, apply the same criteria used for the inherent presumed trustworthiness of public records
  - ARM is a field unto itself and should be studied by forensics folk

Management Analytics

Outline

- Background and problems
- Digital diplomatics vs. Forensics vs. Digital forensics and cases
- Resolution
- Implications and a path forward
- Discussion

Management Analytics

Thank You

http://all.net/ - fc at all.net