

Supporting the Cyber Analytic Process using Visual History on Large Displays

Ankit Singh, Alex Endert, Christopher Andrews, Lauren
Bradel, Robert Kincaid, Chris North

Virginia Tech

Agilent Laboratories

Overview

- Cyber Analytic Process
 - Benefits provide by large displays
- Visual History Design and Prototype
- Lessons Learned, Future Work

Large, High-Resolution Displays

- Personal Workspace
- Single Workstation
- Familiar OS, tools, ...
- Provides additional size, resolution to support analysts



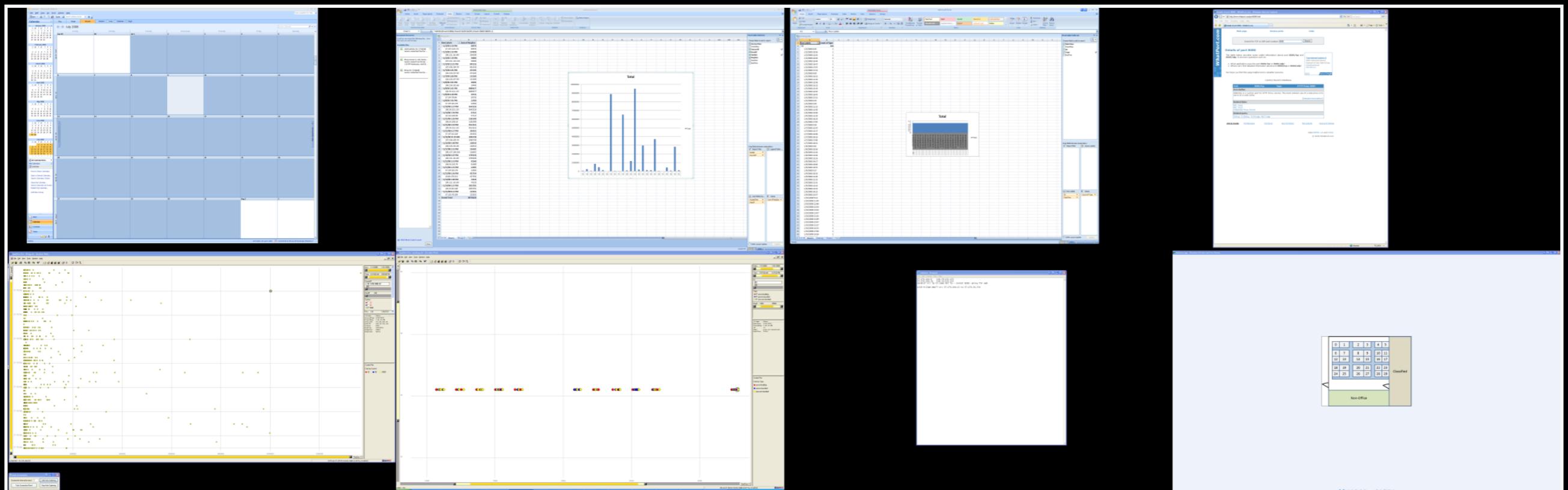
Cyber Analytic Process

- Interviewed 8 professional cyber analysts
- Observed 4 analysts analyze the 2009 VAST Challenge Dataset
 - Simulated Network Flows and Employee Building Access logs



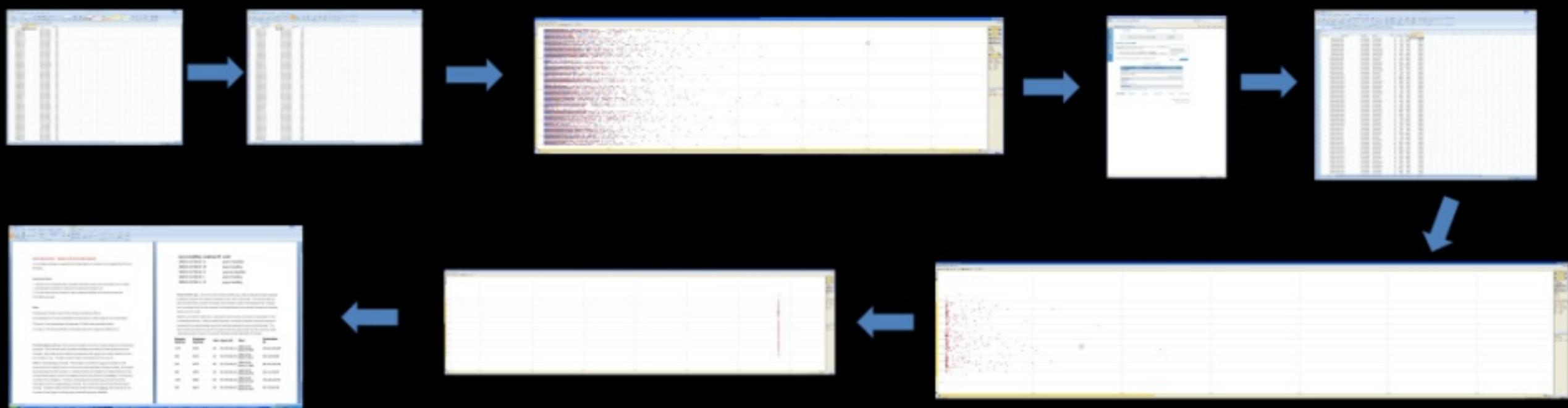
Cyber Analytic Process

- Multiple data sources
- Multiple tools/windows
- Extensive Excel usage



Cyber Analytic Process

- Versioning of files based on hypotheses
 - E.g., v1.1, v1.2, v2.1, ...
 - Reasons: save the data, save the view
- Difficult to re-create process to support findings at time of creating report



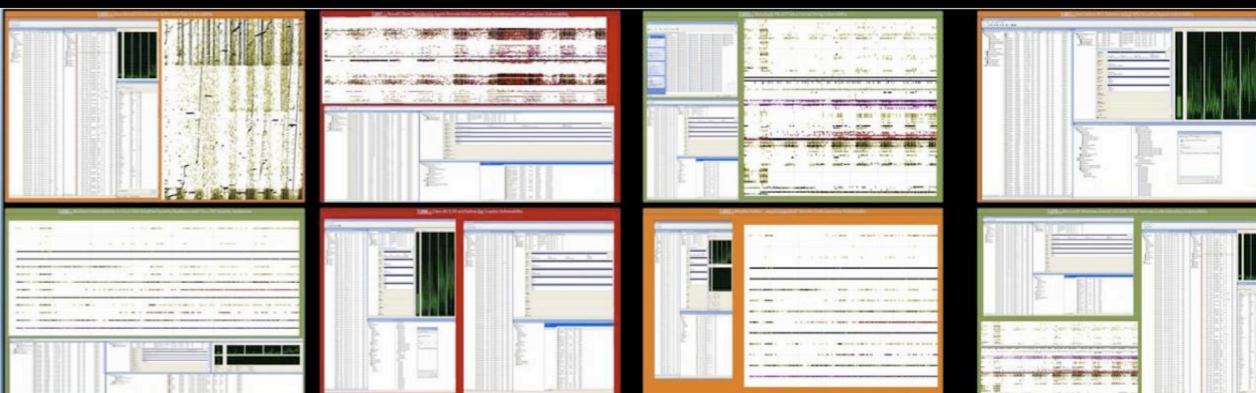
Challenge

- How to design workspaces to support the complex cyber analytic process?

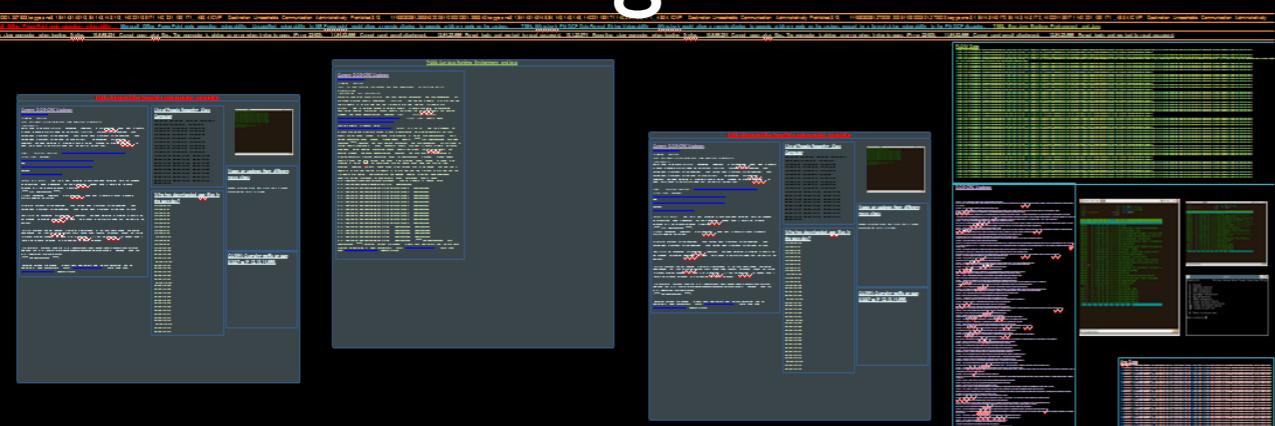
More Resolution and Size



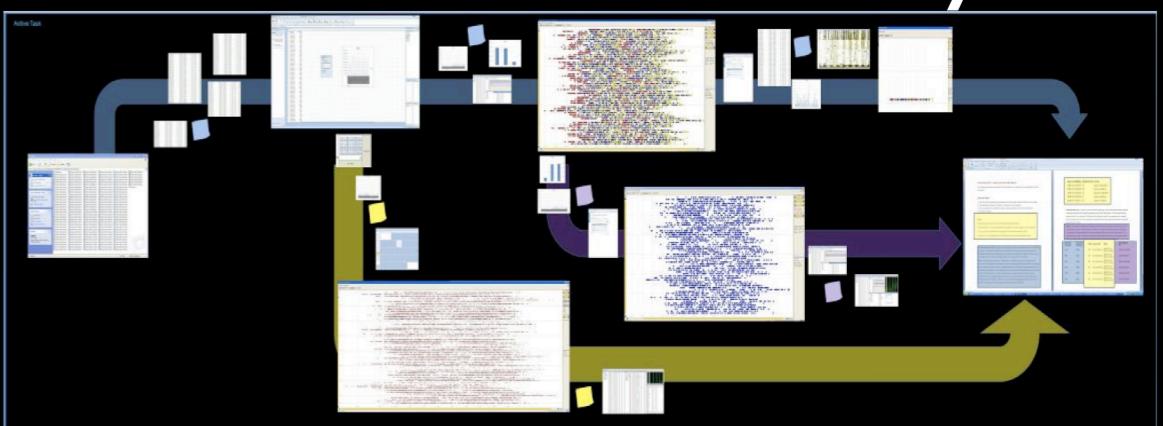
De-Aggregation of Data



Case Management



Process History

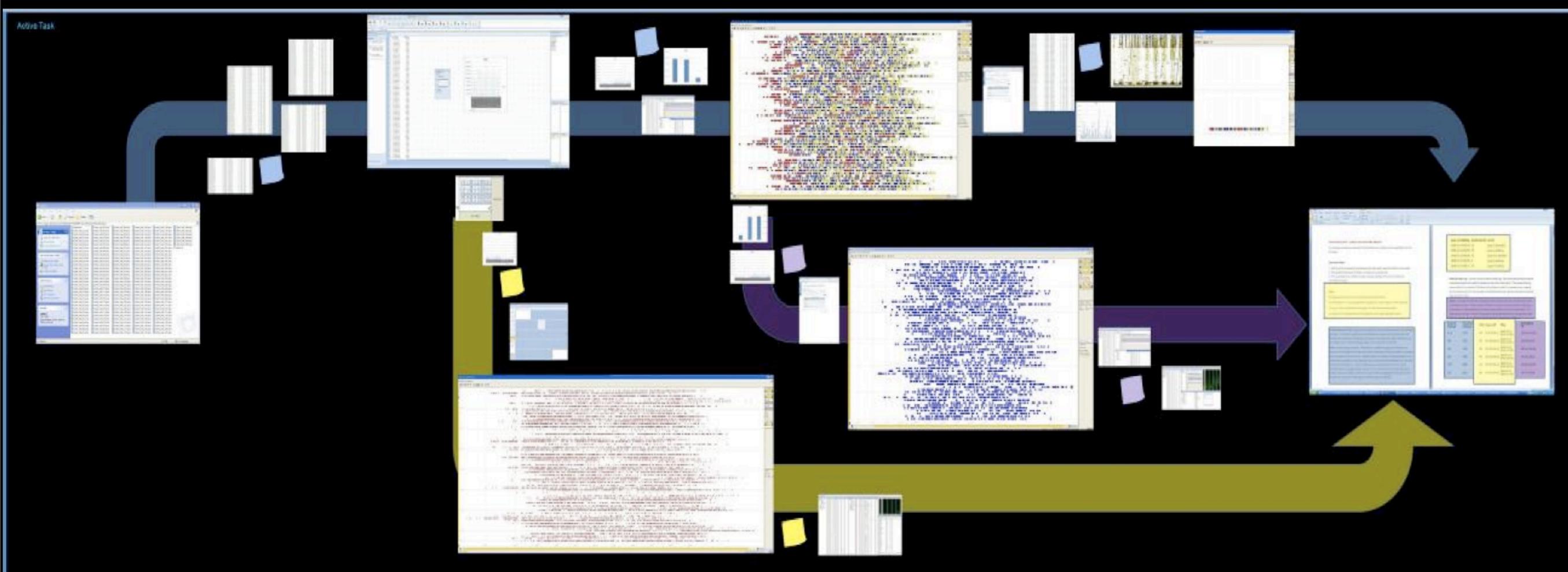


Visual History: Design

Branching

Multiple
Windows, File
Versions

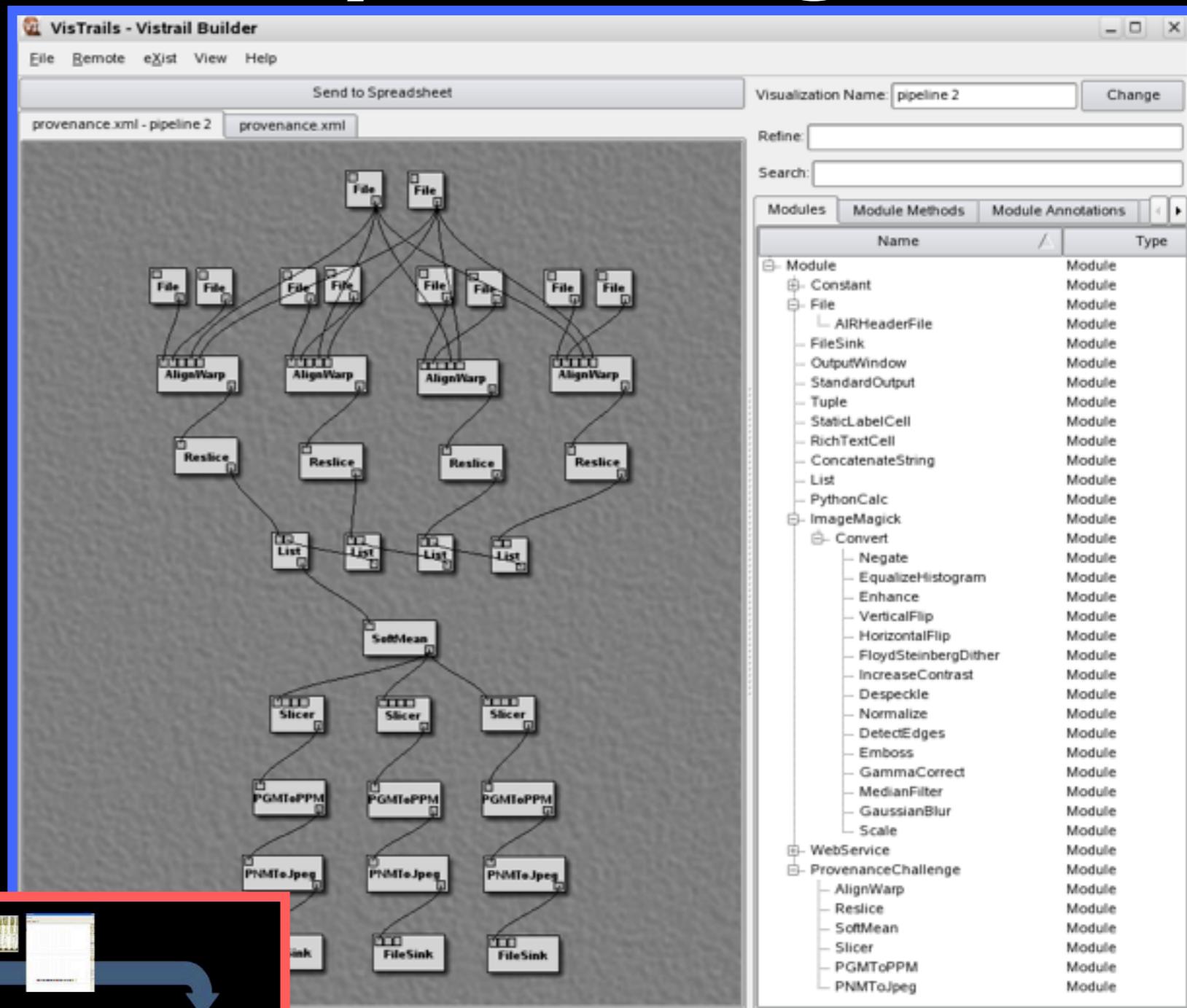
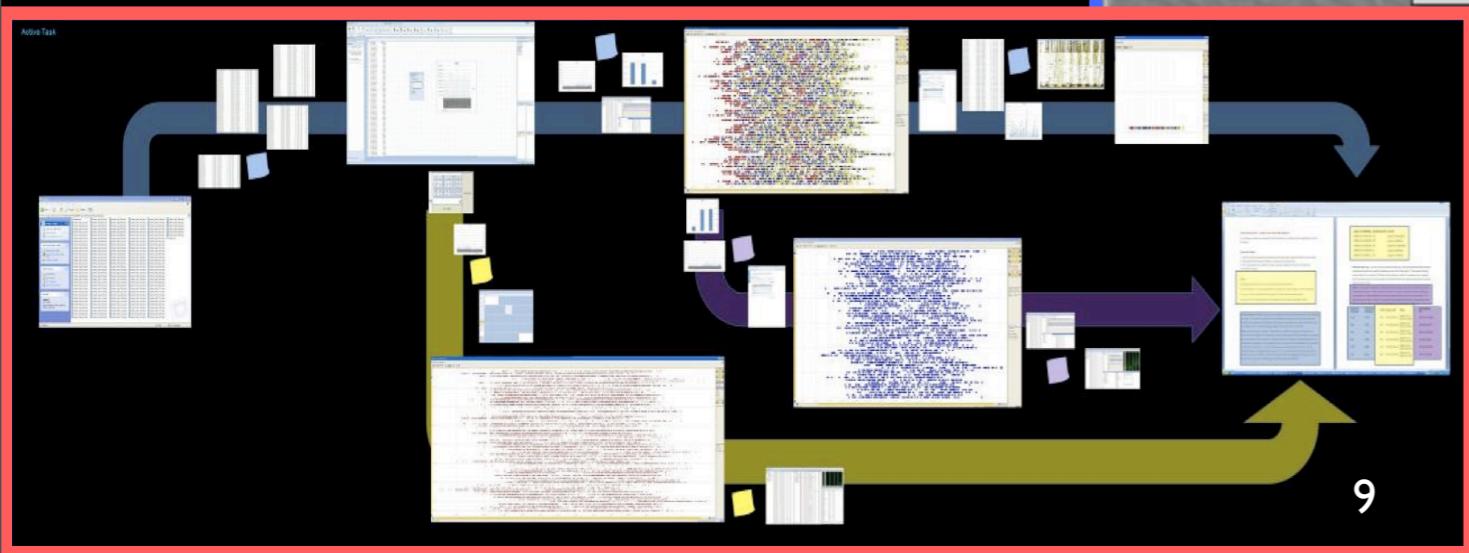
Process
Traceability



Visual History: Design

Visualization of workflow

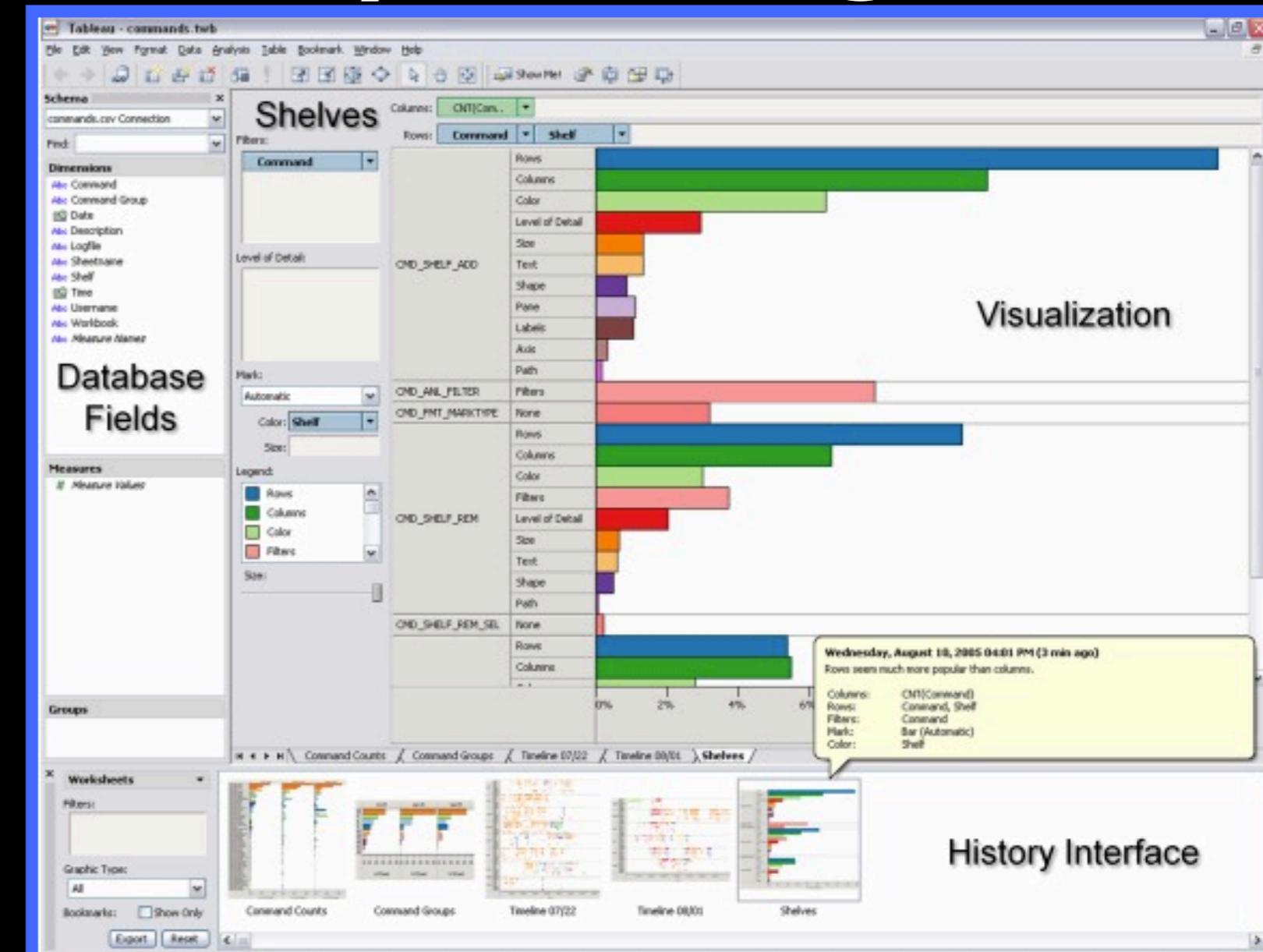
Process integrated in workspace



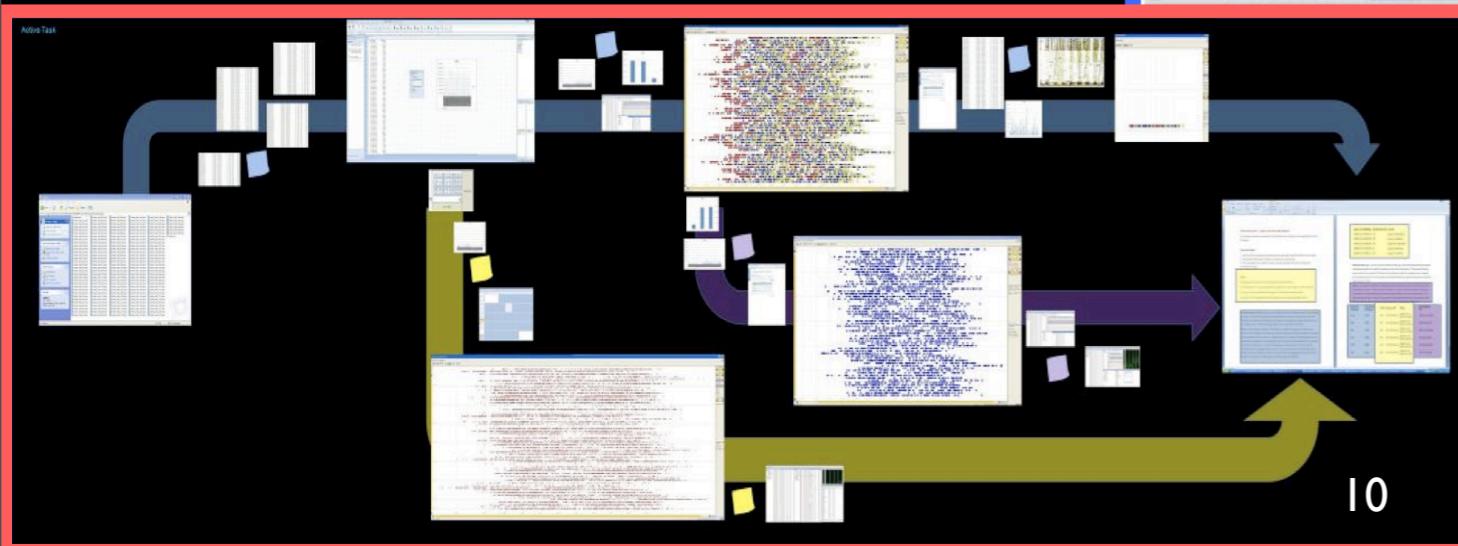
Visual History: Design

History stored away
in thumbnails

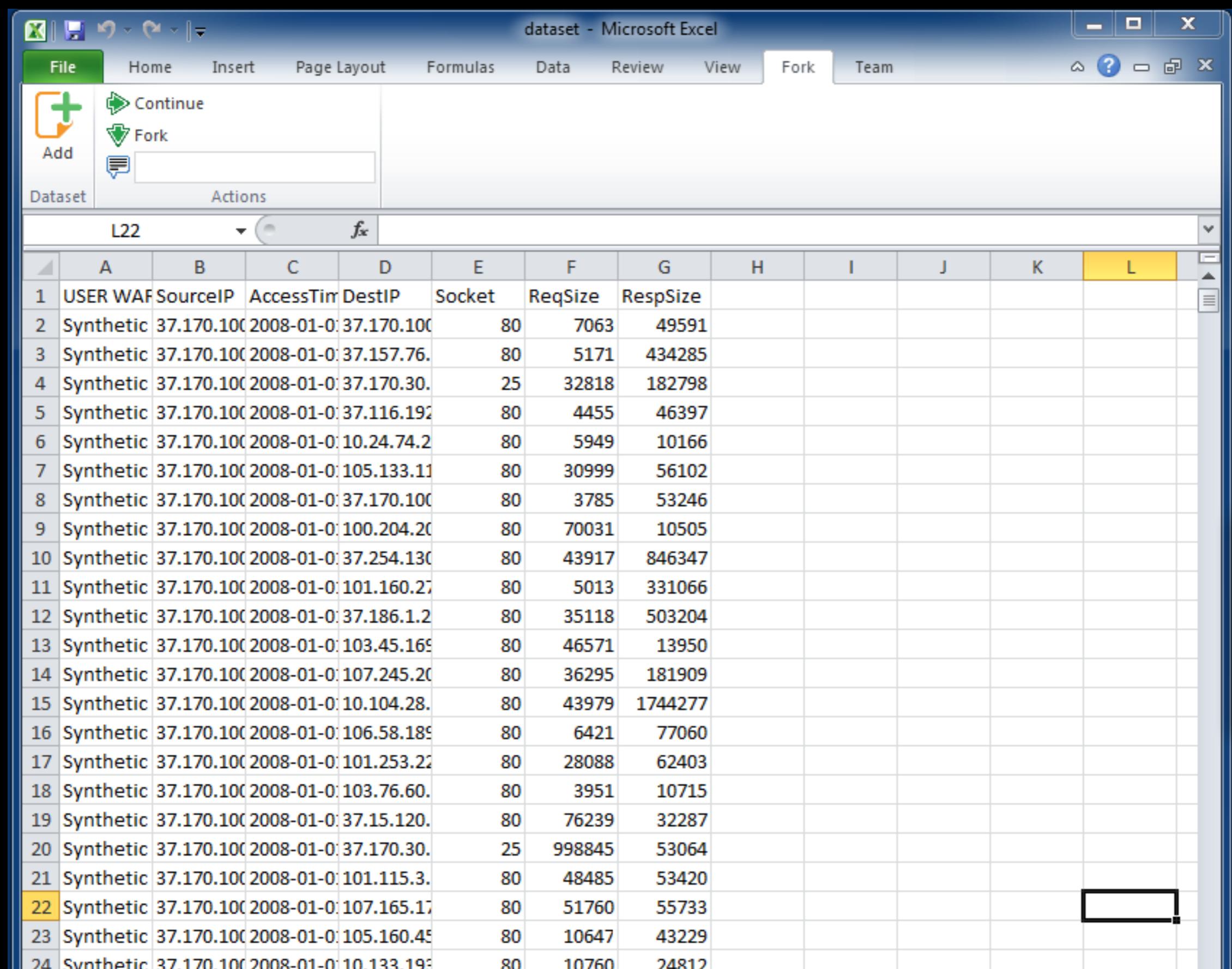
Process integrated
in workspace



Tableau, image from <http://hci.stanford.edu/jheer/files/jheer-thesis.pdf>



Visual History: Implementation



A screenshot of Microsoft Excel showing a dataset titled "dataset - Microsoft Excel". The Excel interface includes a ribbon with tabs: File, Home, Insert, Page Layout, Formulas, Data, Review, View, Fork, and Team. The "Fork" tab is selected. On the left, there's a sidebar with icons for "Add" (orange plus), "Continue" (green arrow), and "Fork" (green downward arrow). Below the sidebar are buttons for "Dataset" and "Actions". The main area displays a table with 24 rows of data. The columns are labeled A through L. The first row contains column headers: "USER WAF SourceIP AccessTim DestIP Socket ReqSize RespSize". Rows 2 through 24 are labeled "Synthetic" and show various network access details. Row 24 is highlighted with a yellow background.

	A	B	C	D	E	F	G	H	I	J	K	L
1	USER WAF	SourceIP	AccessTim	DestIP	Socket	ReqSize	RespSize					
2	Synthetic	37.170.100	2008-01-0	37.170.100	80	7063	49591					
3	Synthetic	37.170.100	2008-01-0	37.157.76.	80	5171	434285					
4	Synthetic	37.170.100	2008-01-0	37.170.30.	25	32818	182798					
5	Synthetic	37.170.100	2008-01-0	37.116.192	80	4455	46397					
6	Synthetic	37.170.100	2008-01-0	10.24.74.2	80	5949	10166					
7	Synthetic	37.170.100	2008-01-0	105.133.11	80	30999	56102					
8	Synthetic	37.170.100	2008-01-0	37.170.100	80	3785	53246					
9	Synthetic	37.170.100	2008-01-0	100.204.20	80	70031	10505					
10	Synthetic	37.170.100	2008-01-0	37.254.130	80	43917	846347					
11	Synthetic	37.170.100	2008-01-0	101.160.27	80	5013	331066					
12	Synthetic	37.170.100	2008-01-0	37.186.1.2	80	35118	503204					
13	Synthetic	37.170.100	2008-01-0	103.45.169	80	46571	13950					
14	Synthetic	37.170.100	2008-01-0	107.245.20	80	36295	181909					
15	Synthetic	37.170.100	2008-01-0	10.104.28.	80	43979	1744277					
16	Synthetic	37.170.100	2008-01-0	106.58.189	80	6421	77060					
17	Synthetic	37.170.100	2008-01-0	101.253.22	80	28088	62403					
18	Synthetic	37.170.100	2008-01-0	103.76.60.	80	3951	10715					
19	Synthetic	37.170.100	2008-01-0	37.15.120.	80	76239	32287					
20	Synthetic	37.170.100	2008-01-0	37.170.30.	25	998845	53064					
21	Synthetic	37.170.100	2008-01-0	101.115.3.	80	48485	53420					
22	Synthetic	37.170.100	2008-01-0	107.165.17	80	51760	55733					
23	Synthetic	37.170.100	2008-01-0	105.160.45	80	10647	43229					
24	Synthetic	37.170.100	2008-01-0	10.133.193	80	10760	24812					

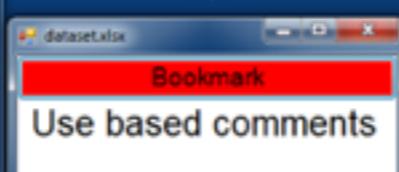
Visual History: Implementation

Branching

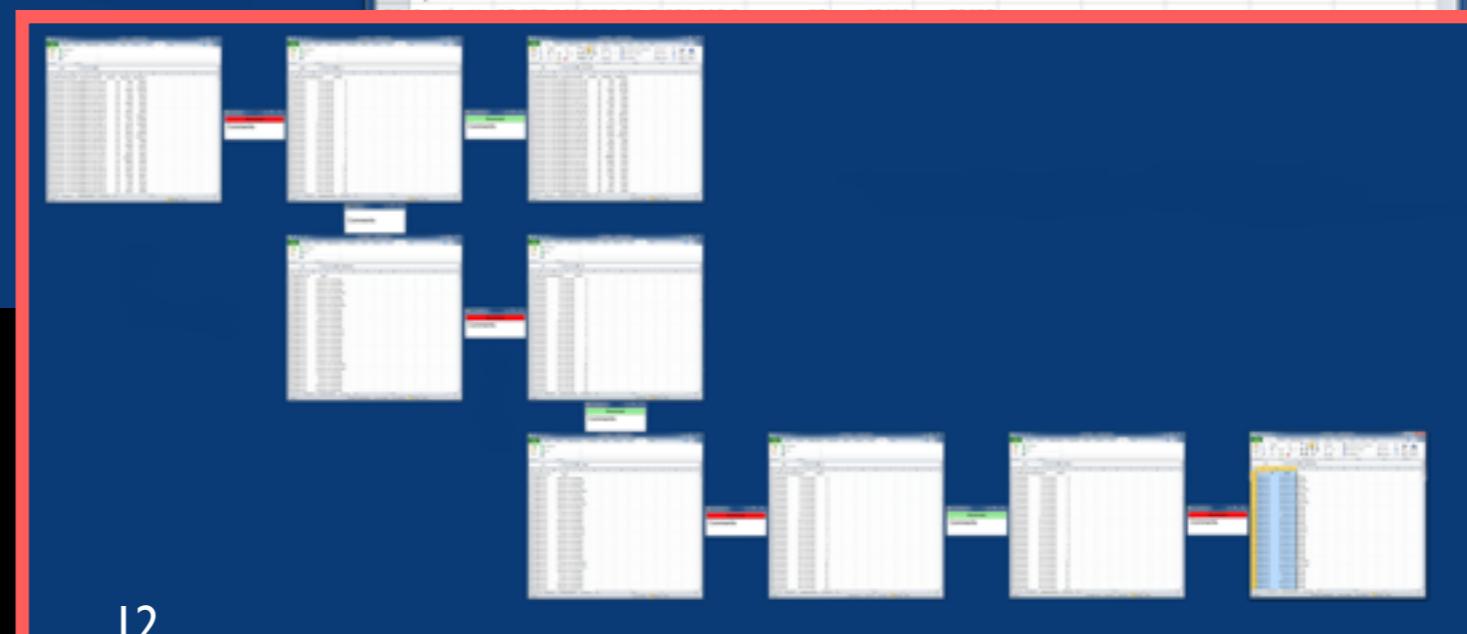
**Multiple Windows,
File Versions**

**Process
Traceability**

1	USER	WAF	SourceIP	AccessTim	DestIP	Socket	ReqSize	RespSize
2	Synthetic	37.170.10X	2008-01-0	37.170.10X	80	7063	49591	
3	Synthetic	37.170.10X	2008-01-0	37.157.76.	80	5171	434285	
4	Synthetic	37.170.10X	2008-01-0	37.170.30.	25	32818	182798	
5	Synthetic	37.170.10X	2008-01-0	37.116.192	80	4455	46397	
6	Synthetic	37.170.10X	2008-01-0	10.24.74.2	80	5949	10166	
7	Synthetic	37.170.10X	2008-01-0	105.133.11	80	30999	56102	
8	Synthetic	37.170.10X	2008-01-0	37.170.10X	80	3785	53246	
9	Synthetic	37.170.10X	2008-01-0	100.204.2f	80	70031	10505	
10	Synthetic	37.170.10X	2008-01-0	37.254.13C	80	43917	846347	
11	Synthetic	37.170.10X	2008-01-0	101.160.27	80	5013	331066	
12	Synthetic	37.170.10X	2008-01-0	37.186.1.2	80	35118	503204	
13	Synthetic	37.170.10X	2008-01-0	103.45.165	80	46571	13950	
14	Synthetic	37.170.10X	2008-01-0	107.245.2f	80	36295	181909	
15	Synthetic	37.170.10X	2008-01-0	10.104.28.	80	43979	1744277	
16	Synthetic	37.170.10X	2008-01-0	106.58.185	80	6421	77060	
17	Synthetic	37.170.10X	2008-01-0	101.253.2f	80	28088	62403	
18	Synthetic	37.170.10X	2008-01-0	103.76.60.	80	3951	10715	
19	Synthetic	37.170.10X	2008-01-0	37.15.120.	80	76239	32287	
20	Synthetic	37.170.10X	2008-01-0	37.170.30.	25	998845	53064	
21	Synthetic	37.170.10X	2008-01-0	101.115.3.	80	48485	53420	
22	Synthetic	37.170.10X	2008-01-0	107.165.17	80	51760	55733	
23	Synthetic	37.170.10X	2008-01-0	105.160.4f	80	10647	43229	
24	Synthetic	37.170.10X	2008-01-0	10.133.195	80	10760	24812	
25	Synthetic	37.170.10X	2008-01-0	104.233.6f	80	4940	24911	
26	Synthetic	37.170.10X	2008-01-0	101.56.23.	80	4330	33124	
27	Synthetic	37.170.10X	2008-01-0	102.109.2f	80	6837	13402	
28	Synthetic	37.170.10X	2008-01-0	105.141.2f	80	43107	23036	



1	USER	WAF	SourceIP	AccessTim	DestIP	Socket	ReqSize	RespSize
2	Synthetic	37.170.10X	2008-01-0	37.170.10X	80	7063	49591	
3	Synthetic	37.170.10X	2008-01-0	37.157.76.	80	5171	434285	
4	Synthetic	37.170.10X	2008-01-0	37.170.30.	25	32818	182798	
5	Synthetic	37.170.10X	2008-01-0	37.116.192	80	4455	46397	
6	Synthetic	37.170.10X	2008-01-0	10.24.74.2	80	5949	10166	
7	Synthetic	37.170.10X	2008-01-0	105.133.11	80	30999	56102	
8	Synthetic	37.170.10X	2008-01-0	37.170.10X	80	3785	53246	
9	Synthetic	37.170.10X	2008-01-0	100.204.2f	80	70031	10505	
10	Synthetic	37.170.10X	2008-01-0	37.254.13C	80	43917	846347	
11	Synthetic	37.170.10X	2008-01-0	101.160.27	80	5013	331066	
12	Synthetic	37.170.10X	2008-01-0	37.186.1.2	80	35118	503204	
13	Synthetic	37.170.10X	2008-01-0	103.45.165	80	46571	13950	
14	Synthetic	37.170.10X	2008-01-0	107.245.2f	80	36295	181909	
15	Synthetic	37.170.10X	2008-01-0	10.104.28.	80	43979	1744277	
16	Synthetic	37.170.10X	2008-01-0	106.58.185	80	6421	77060	
17	Synthetic	37.170.10X	2008-01-0	101.253.2f	80	28088	62403	
18	Synthetic	37.170.10X	2008-01-0	103.76.60.	80	3951	10715	
19	Synthetic	37.170.10X	2008-01-0	37.15.120.	80	76239	32287	
20	Synthetic	37.170.10X	2008-01-0	37.170.30.	25	998845	53064	

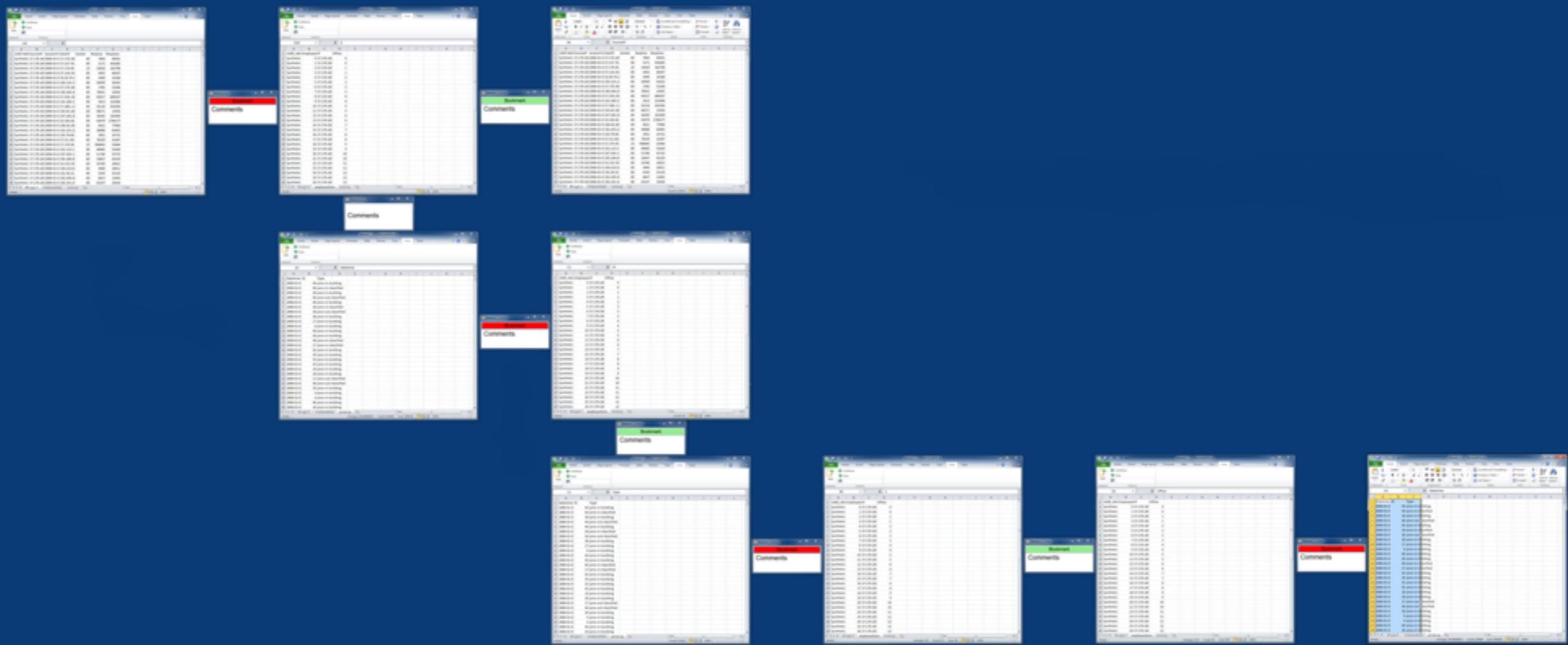


Visual History: Implementation

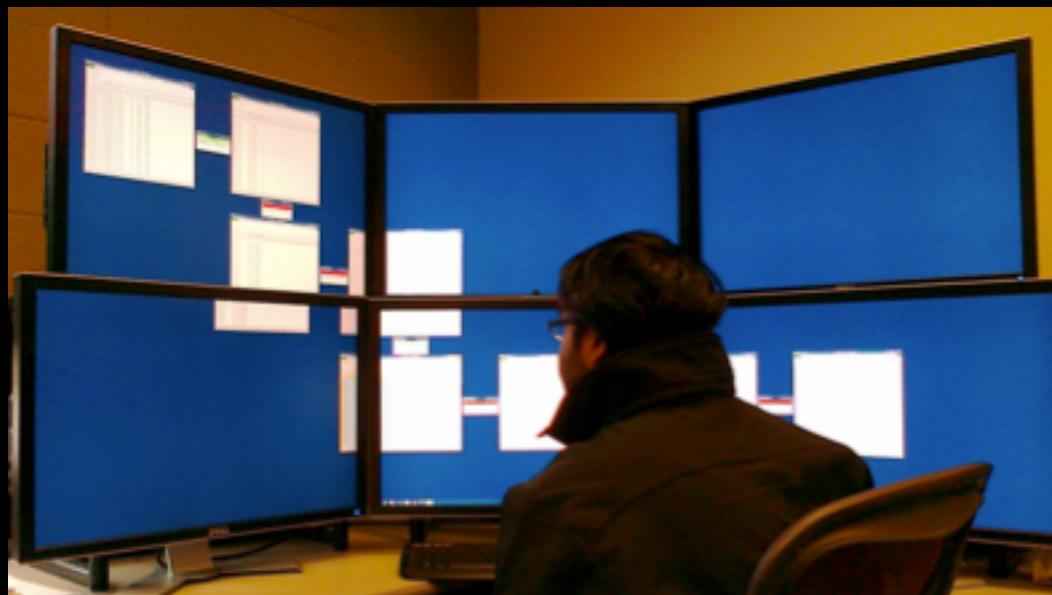
Branching

Multiple Windows,
File Versions

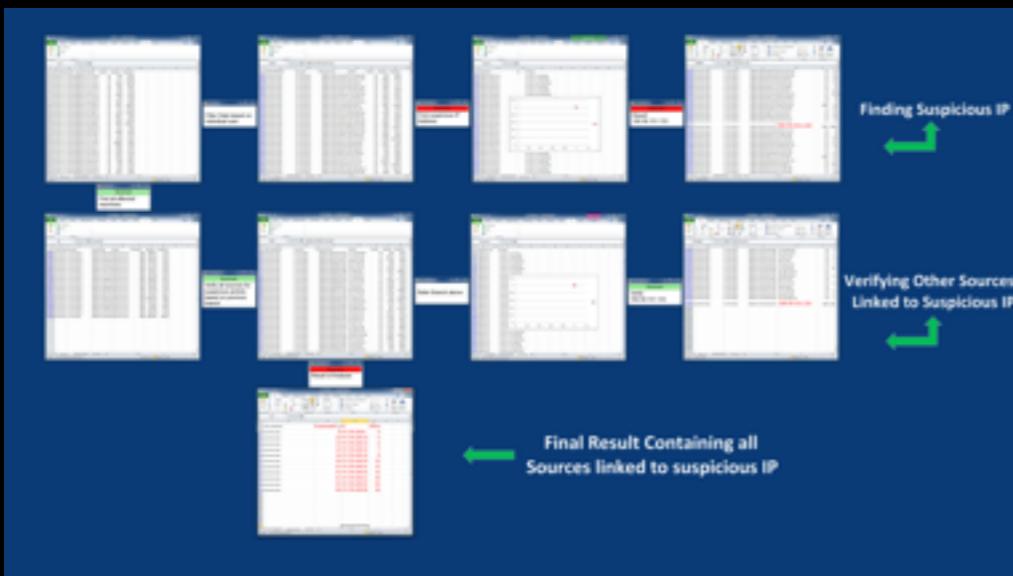
Process Traceability



Visual History: Use Case



- 2009 VAST Challenge Dataset
- Simulated Network Flows and Employee Building Access logs



- Explore features in realistic scenario

Visual History: Implementation

Branching

Multiple Windows,
File Versions

Process
Traceability

EmployeeID	IP	Office
1	192.168.1.100	A
2	192.168.1.101	B
3	192.168.1.102	C
4	192.168.1.103	D
5	192.168.1.104	E
6	192.168.1.105	F
7	192.168.1.106	G
8	192.168.1.107	H
9	192.168.1.108	I
10	192.168.1.109	J
11	192.168.1.110	K
12	192.168.1.111	L
13	192.168.1.112	M
14	192.168.1.113	N
15	192.168.1.114	O
16	192.168.1.115	P
17	192.168.1.116	Q
18	192.168.1.117	R
19	192.168.1.118	S
20	192.168.1.119	T
21	192.168.1.120	U
22	192.168.1.121	V
23	192.168.1.122	W
24	192.168.1.123	X
25	192.168.1.124	Y
26	192.168.1.125	Z
27	192.168.1.126	A
28	192.168.1.127	B
29	192.168.1.128	C
30	192.168.1.129	D
31	192.168.1.130	E
32	192.168.1.131	F
33	192.168.1.132	G
34	192.168.1.133	H
35	192.168.1.134	I
36	192.168.1.135	J
37	192.168.1.136	K
38	192.168.1.137	L
39	192.168.1.138	M
40	192.168.1.139	N
41	192.168.1.140	O
42	192.168.1.141	P
43	192.168.1.142	Q
44	192.168.1.143	R
45	192.168.1.144	S
46	192.168.1.145	T
47	192.168.1.146	U
48	192.168.1.147	V
49	192.168.1.148	W
50	192.168.1.149	X
51	192.168.1.150	Y
52	192.168.1.151	Z
53	192.168.1.152	A
54	192.168.1.153	B
55	192.168.1.154	C
56	192.168.1.155	D
57	192.168.1.156	E
58	192.168.1.157	F
59	192.168.1.158	G
60	192.168.1.159	H
61	192.168.1.160	I
62	192.168.1.161	J
63	192.168.1.162	K
64	192.168.1.163	L
65	192.168.1.164	M
66	192.168.1.165	N
67	192.168.1.166	O
68	192.168.1.167	P
69	192.168.1.168	Q
70	192.168.1.169	R
71	192.168.1.170	S
72	192.168.1.171	T
73	192.168.1.172	U
74	192.168.1.173	V
75	192.168.1.174	W
76	192.168.1.175	X
77	192.168.1.176	Y
78	192.168.1.177	Z
79	192.168.1.178	A
80	192.168.1.179	B
81	192.168.1.180	C
82	192.168.1.181	D
83	192.168.1.182	E
84	192.168.1.183	F
85	192.168.1.184	G
86	192.168.1.185	H
87	192.168.1.186	I
88	192.168.1.187	J
89	192.168.1.188	K
90	192.168.1.189	L
91	192.168.1.190	M
92	192.168.1.191	N
93	192.168.1.192	O
94	192.168.1.193	P
95	192.168.1.194	Q
96	192.168.1.195	R
97	192.168.1.196	S
98	192.168.1.197	T
99	192.168.1.198	U
100	192.168.1.199	V
101	192.168.1.200	W
102	192.168.1.201	X
103	192.168.1.202	Y
104	192.168.1.203	Z
105	192.168.1.204	A
106	192.168.1.205	B
107	192.168.1.206	C
108	192.168.1.207	D
109	192.168.1.208	E
110	192.168.1.209	F
111	192.168.1.210	G
112	192.168.1.211	H
113	192.168.1.212	I
114	192.168.1.213	J
115	192.168.1.214	K
116	192.168.1.215	L
117	192.168.1.216	M
118	192.168.1.217	N
119	192.168.1.218	O
120	192.168.1.219	P
121	192.168.1.220	Q
122	192.168.1.221	R
123	192.168.1.222	S
124	192.168.1.223	T
125	192.168.1.224	U
126	192.168.1.225	V
127	192.168.1.226	W
128	192.168.1.227	X
129	192.168.1.228	Y
130	192.168.1.229	Z
131	192.168.1.230	A
132	192.168.1.231	B
133	192.168.1.232	C
134	192.168.1.233	D
135	192.168.1.234	E
136	192.168.1.235	F
137	192.168.1.236	G
138	192.168.1.237	H
139	192.168.1.238	I
140	192.168.1.239	J
141	192.168.1.240	K
142	192.168.1.241	L
143	192.168.1.242	M
144	192.168.1.243	N
145	192.168.1.244	O
146	192.168.1.245	P
147	192.168.1.246	Q
148	192.168.1.247	R
149	192.168.1.248	S
150	192.168.1.249	T
151	192.168.1.250	U
152	192.168.1.251	V
153	192.168.1.252	W
154	192.168.1.253	X
155	192.168.1.254	Y
156	192.168.1.255	Z
157	192.168.1.256	A
158	192.168.1.257	B
159	192.168.1.258	C
160	192.168.1.259	D
161	192.168.1.260	E
162	192.168.1.261	F
163	192.168.1.262	G
164	192.168.1.263	H
165	192.168.1.264	I
166	192.168.1.265	J
167	192.168.1.266	K
168	192.168.1.267	L
169	192.168.1.268	M
170	192.168.1.269	N
171	192.168.1.270	O
172	192.168.1.271	P
173	192.168.1.272	Q
174	192.168.1.273	R
175	192.168.1.274	S
176	192.168.1.275	T
177	192.168.1.276	U
178	192.168.1.277	V
179	192.168.1.278	W
180	192.168.1.279	X
181	192.168.1.280	Y
182	192.168.1.281	Z
183	192.168.1.282	A
184	192.168.1.283	B
185	192.168.1.284	C
186	192.168.1.285	D
187	192.168.1.286	E
188	192.168.1.287	F
189	192.168.1.288	G
190	192.168.1.289	H
191	192.168.1.290	I
192	192.168.1.291	J
193	192.168.1.292	K
194	192.168.1.293	L
195	192.168.1.294	M
196	192.168.1.295	N
197	192.168.1.296	O
198	192.168.1.297	P
199	192.168.1.298	Q
200	192.168.1.299	R
201	192.168.1.300	S
202	192.168.1.301	T
203	192.168.1.302	U
204	192.168.1.303	V
205	192.168.1.304	W
206	192.168.1.305	X
207	192.168.1.306	Y
208	192.168.1.307	Z
209	192.168.1.308	A
210	192.168.1.309	B
211	192.168.1.310	C
212	192.168.1.311	D
213	192.168.1.312	E
214	192.168.1.313	F
215	192.168.1.314	G
216	192.168.1.315	H
217	192.168.1.316	I
218	192.168.1.317	J
219	192.168.1.318	K
220	192.168.1.319	L
221	192.168.1.320	M
222	192.168.1.321	N
223	192.168.1.322	O
224	192.168.1.323	P
225	192.168.1.324	Q
226	192.168.1.325	R
227	192.168.1.326	S
228	192.168.1.327	T
229	192.168.1.328	U
230	192.168.1.329	V

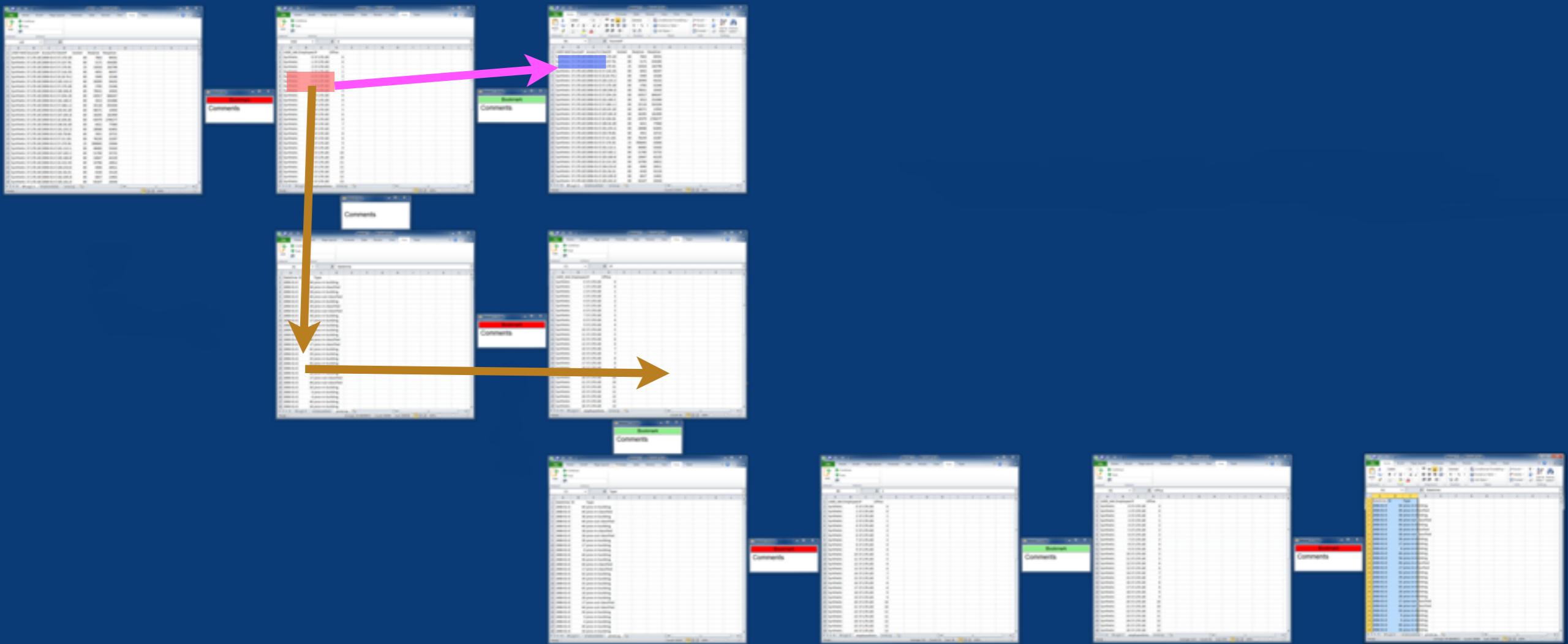
Use Case: Lessons Learned

- Propagating Changes vs. Branching new version
 - Brushing & Linking through Process
- Automatic vs. Manual Layout of History
 - When to fork, branch?
 - Running out of space?

Propagating vs. Forking

Visual History maintains process actively in the workspace.

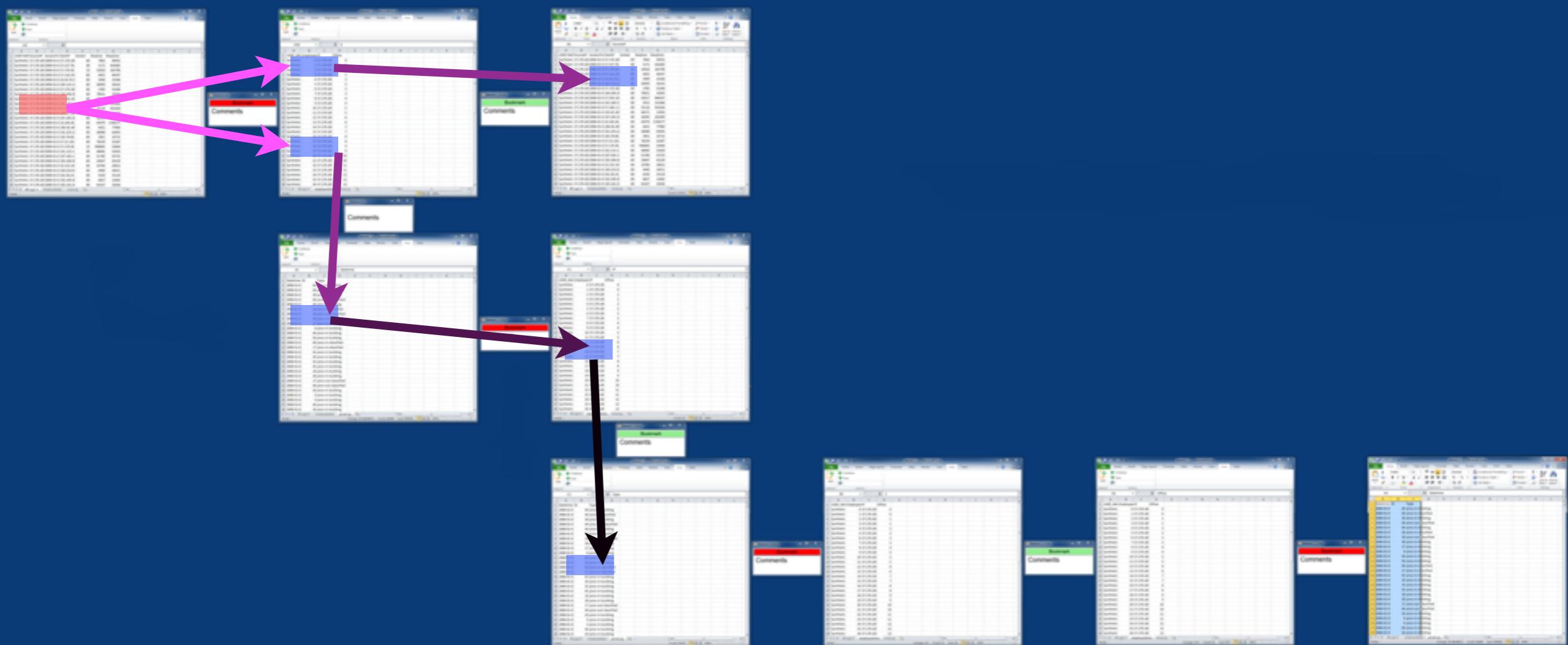
How to adjust workspace when previous states are changed?



Brushing & Linking through Process

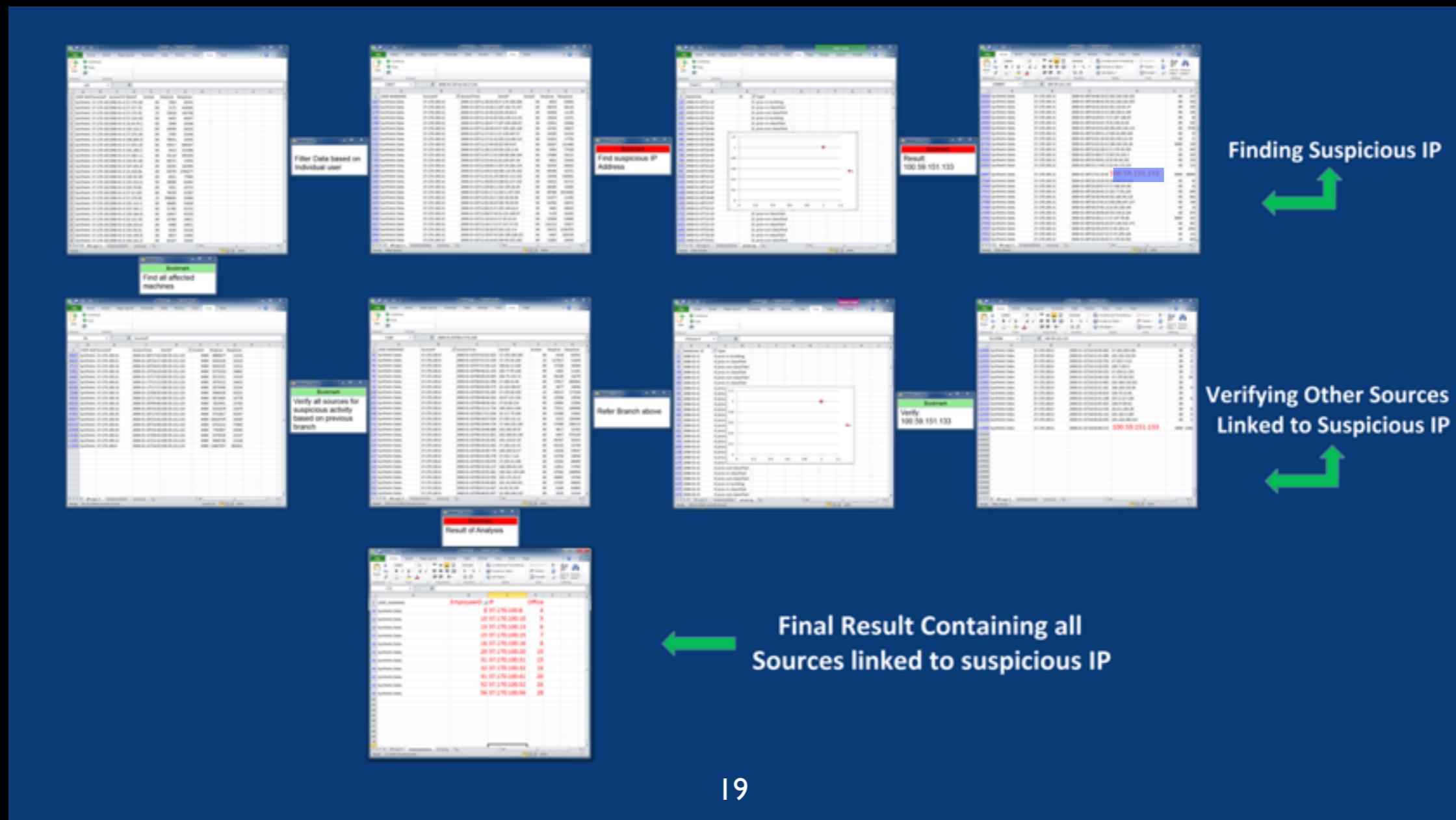
Visual History maintains process actively in the workspace.

How to highlight impacted downstream data?



Automatic vs. Manual Layout

- *Balancing automatic branching with user-defined positioning of windows*
- *How to handle display space limitations?*
- *Scalability of branching*



Future Work

- Evaluate design decisions from lessons learned
- Implementation
- Formal user study evaluation
 - *How does keeping the history current impact the dynamic analytic process of the user?*

Conclusions

- Cyber Analytic Workspaces can support the process of the analyst
 - Combining algorithmic aids (e.g., sniffers, filters, alerts, ...) with human intuition
- With *Visual History*, we merge traditional “history” with “process”
- *Visual History* focuses on the importance of the user process as well as the *solution*

Conclusions

- Cyber Analytic Workspaces can support the process of the analyst
- Combining algorithmic aids (e.g., sniffers, filters, alerts, ...) with human intuition
- With *Visual History*, we merge traditional “history” with “process”
- *Visual History* focuses on the importance of the user process as well as the solution

Thanks!

Questions?