An Automated Timeline Reconstruction Approach for Digital Forensic Investigations

By

Christopher Hargreaves and Jonathan Patterson

Presented At

The Digital Forensic Research Conference

DFRWS 2012 USA Washington, DC (Aug 6th - 8th)

DFRWS is dedicated to the sharing of knowledge and ideas about digital forensics research. Ever since it organized the first open workshop devoted to digital forensics in 2001, DFRWS continues to bring academics and practitioners together in an informal environment. As a non-profit, volunteer organization, DFRWS sponsors technical working groups, annual conferences and challenges to help drive the direction of research and development.

http:/dfrws.org

Cranfield UNIVERSITY

Centre for Forensic Computing

An automated timeline reconstruction approach for digital forensic investigations

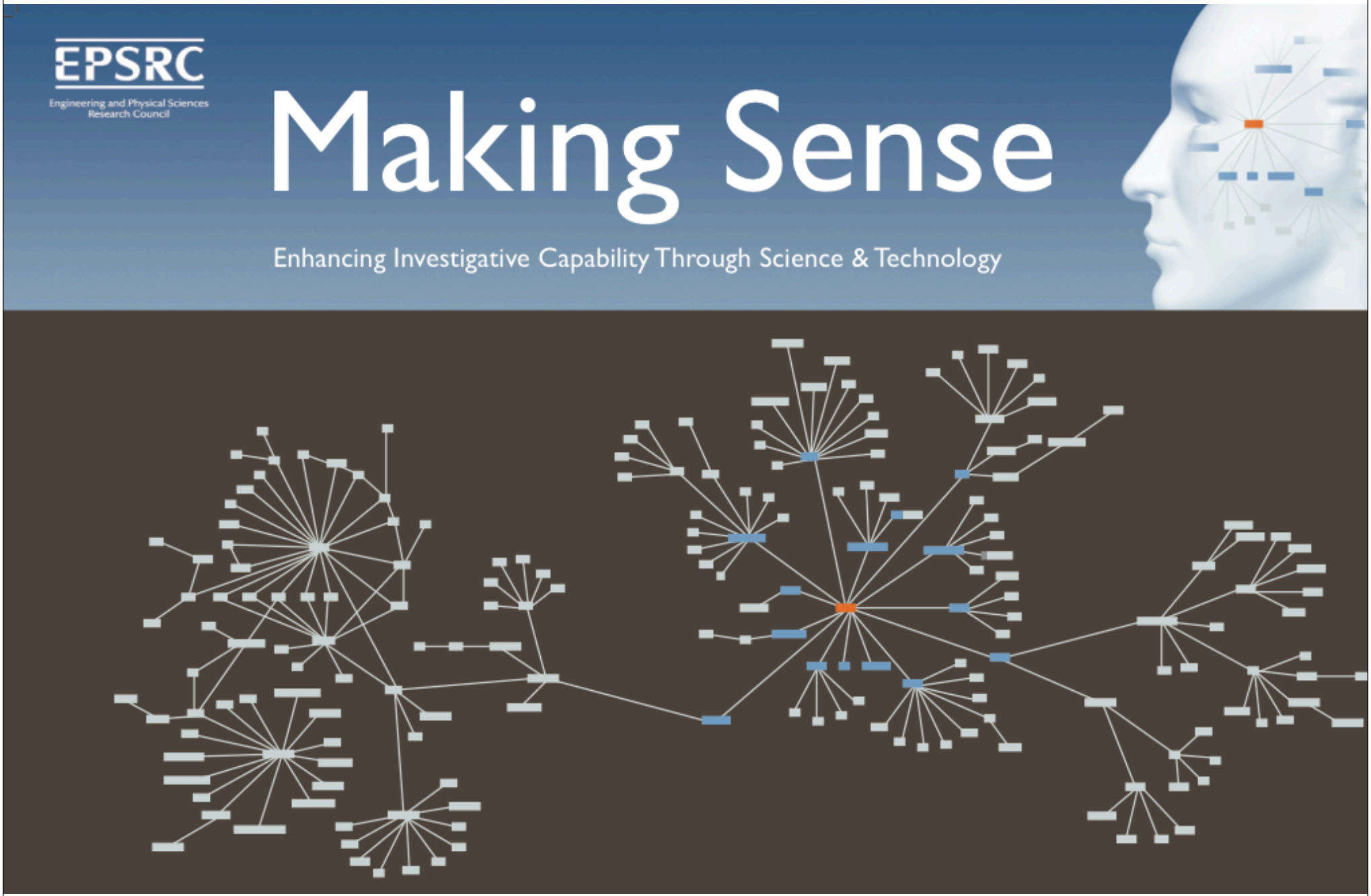
Dr Chris Hargreaves & Jony Patterson

EPSRC

Engineering and Physical Sciences Research Council

Making Sense

Enhancing Investigative Capability Through Science & Technology



Research Aim

- Part of the project is concerned with providing a ‘gist’ of various data sources
  - documents
  - images
  - videos

Research Aim

- What is the ‘gist’ of a hard drive?
  - gallery view of pictures
  - proportion of the disk that are system files, images, videos etc.
  - list of email addresses
  - ...

Summary of a hard drive?

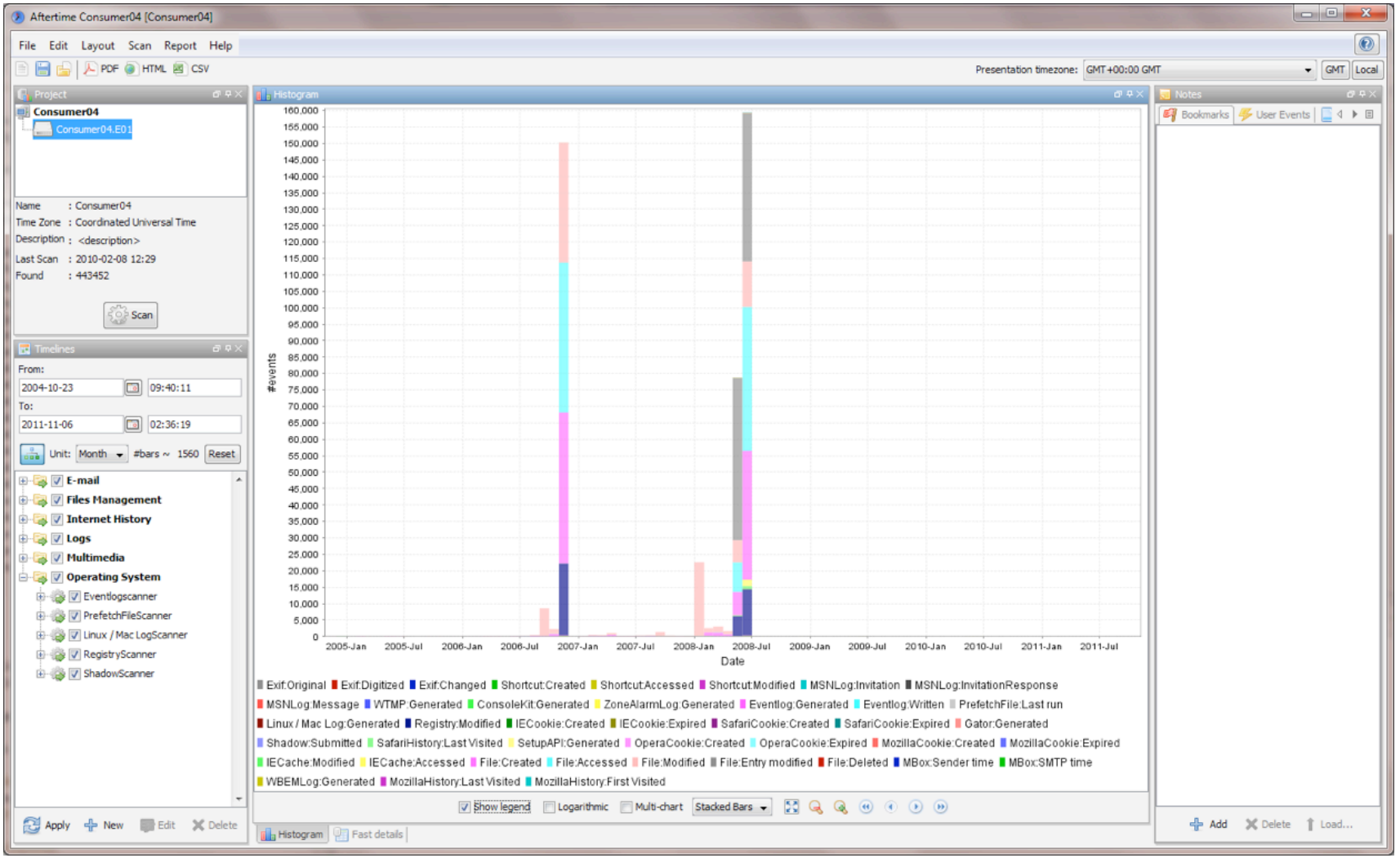
"what is the event history of this computer?"

Research Aim Summary

- Needs to provide a ‘gist’ - a ‘summary of activity on the disk’
- Need an event reconstruction tool that produces ‘human understandable events’
- Needs to satisfy forensic requirements, particularly traceability, repeatability
- Needs to be extensible, i.e. allow the community to add
  - EnScript, RegRipper, Volatility

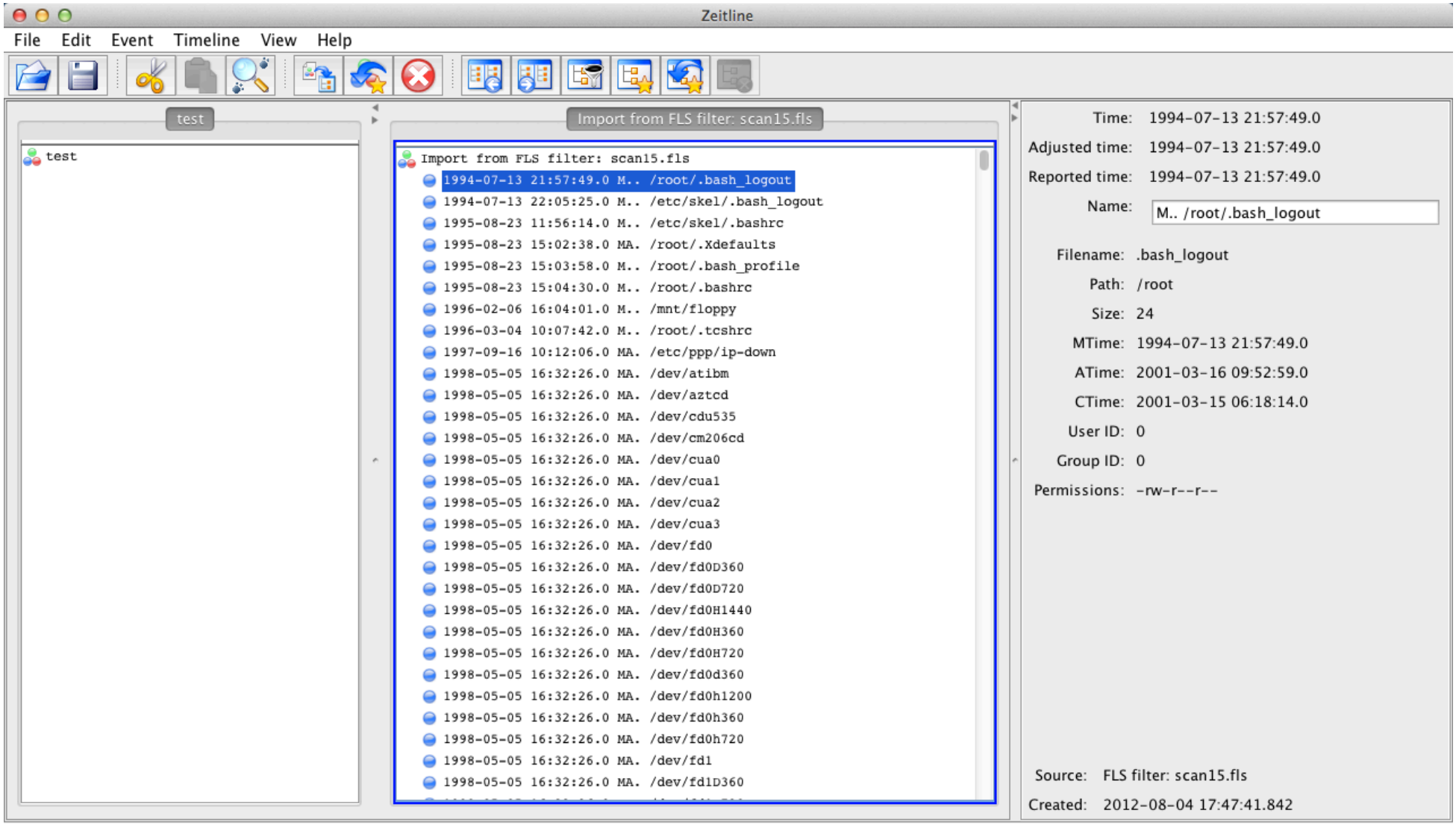
Existing timeline tools

Aftertime



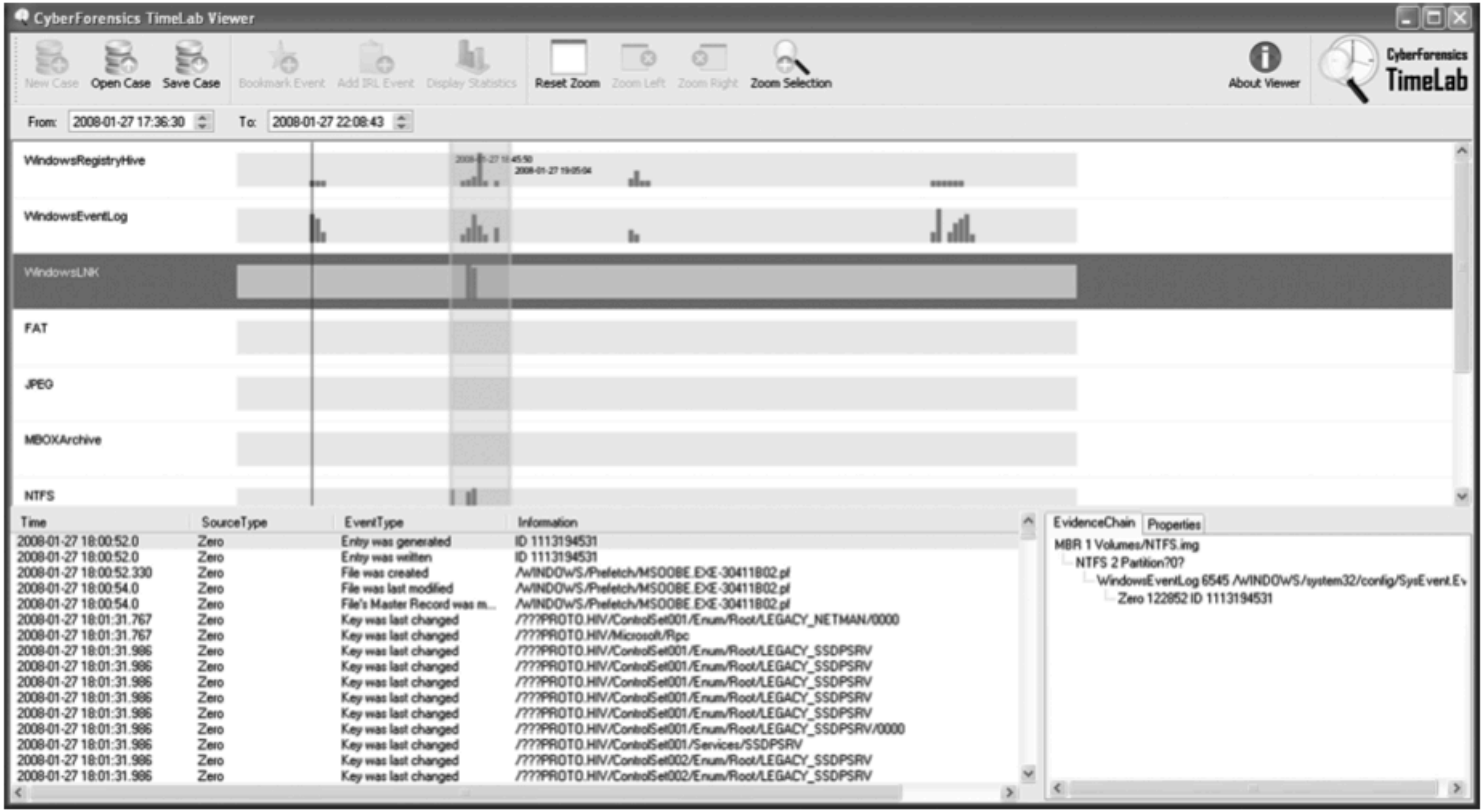
Netherlands Forensic Institute (NFI Labs). 2005. Aftertime, http:www.holmes.nl/NFIlabs/Aftertime/index.html;

Zeitline



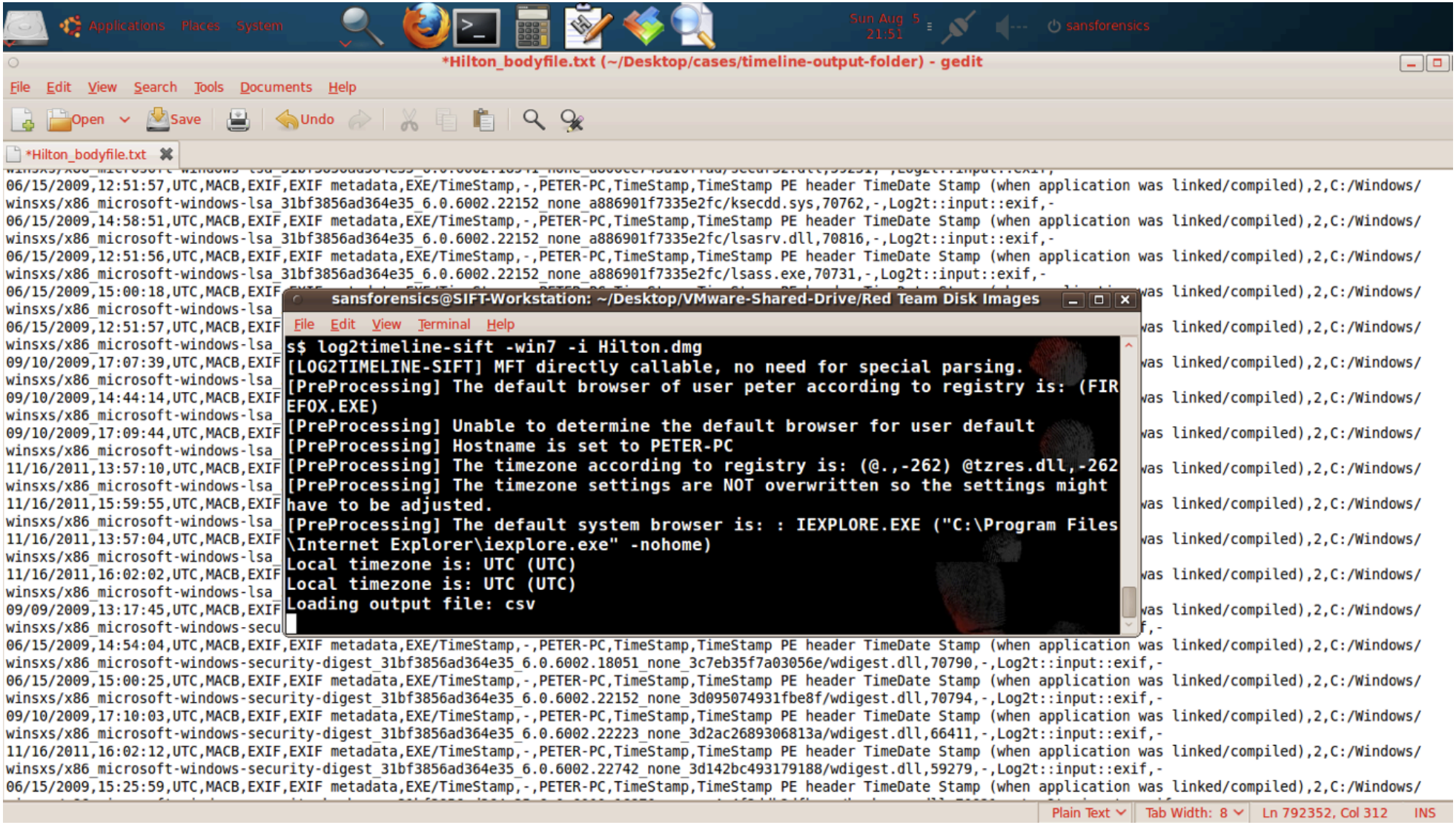
Buchholz, F. & Falk, C., 2005. Design and Implementation of Zeitline: a Forensic Timeline Editor. *Digital Forensics Research Workshop*.

Existing Work on Timelines: Cyber Forensic Time Lab (CFTL)



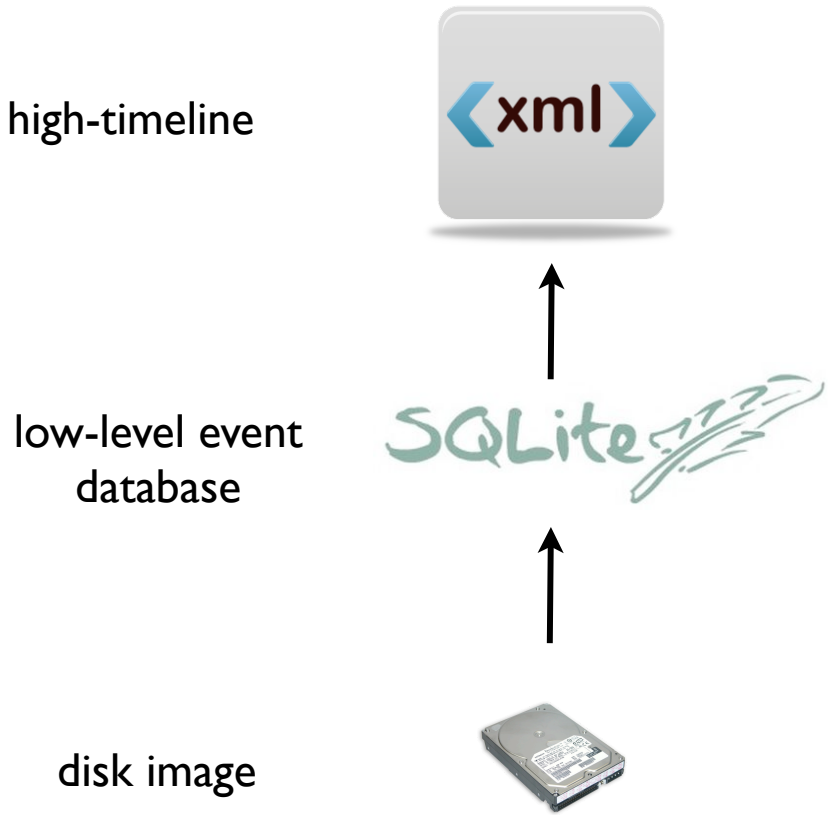
Olsson, J. & Boldt, M., 2009. Computer forensic timeline visualization tool. Digital Investigation, 6(Supplement 1), pp.S78–S87.

log2timeline



Guðjónsson, K., 2010. Mastering the Super Timeline with log2timeline. pp.1–84.

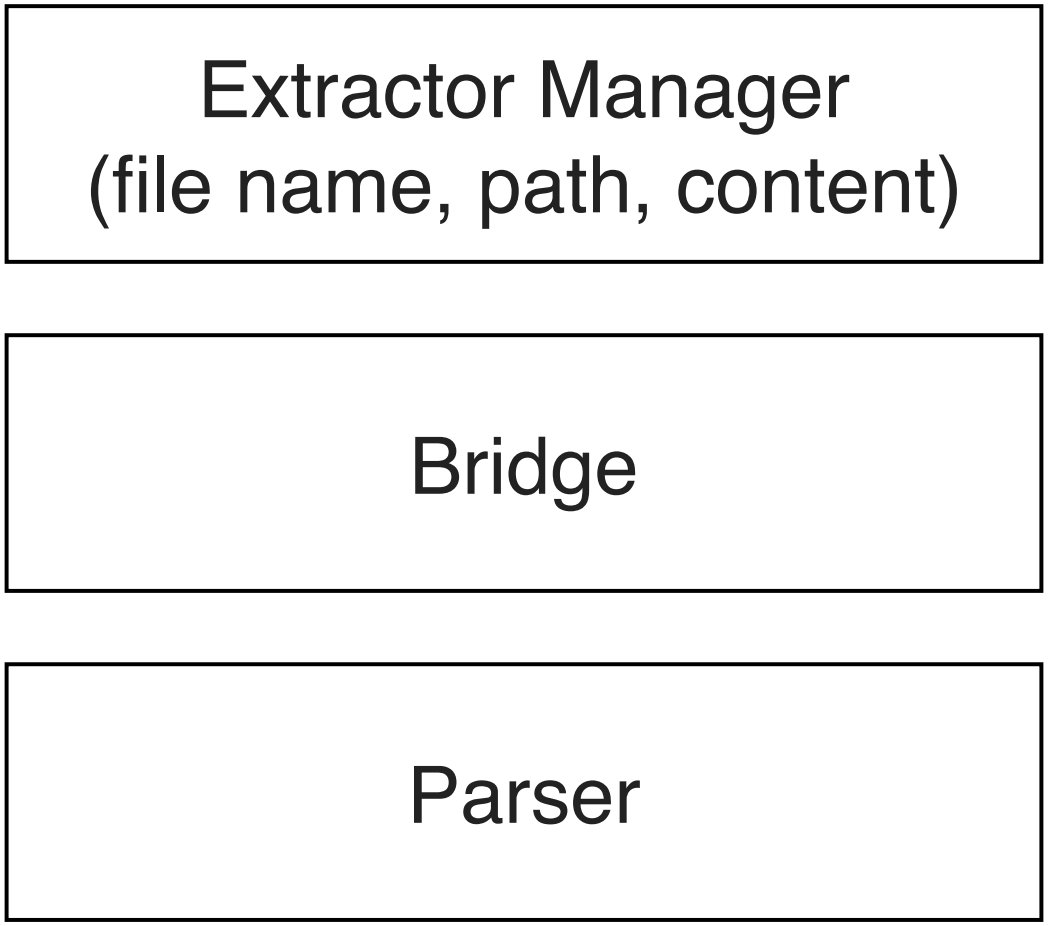
Overview of our approach



Software Components

- **Low level events**
- **Low level timelines**
- **High level events**
- **High level timelines**
- Case management
- Time converters
- File system/disk image access
- Utilities e.g logging

Low-level time extraction



Extractor Manager can match on file name/path

```
elif file_name_and_path[-11:] == "_CACHE_MAP_":
    logging.debug("%s is a Firefox Cache Map. Running parser..."
                                                    % file_name_and_path)
    firefox_extractor = FirefoxCacheBridge.FirefoxCacheTimeExtractor(file_name_and_path,
                                                                     mount_path, evidence)
    firefox_event_timeline = firefox_extractor.GetTimes()
    logging.debug("Extracted %d events from %s" % (len(firefox_event_timeline),
                                                   file_name_and_path))
    return firefox_event_timeline
```

Extractor Manager can match on file signature

```
elif file_header[0:4] == b"\xFF\xD8\xFF\xE1" or file_header[0:4] == b"\xFF\xD8\xFF\xE0":
    logging.debug("TimeExtractor found an jpg file (%s)" % file_name_and_path)
    jpg_file_extractor = EXIFBridge.EXIFTimeExtractor(file_name_and_path,
                                                      mount_path, evidence)
    jpg_file_event_timeline = jpg_file_extractor.GetTimes()
    logging.debug("Extracted %d events from %s" % (len(jpg_file_event_timeline),
                                                   file_name_and_path))
    return jpg_file_event_timeline
```

Low-level event format

id	258920
min_date_time	1301136207.4043
max_date_time	1301136207.4043
evidence	CH-TestImage2
plugin	Registry Parser
type	Last Updated
path	/Software/Microsoft/Internet Explorer/ TypedURLs
device	CH-TestImage2
keys	(“url1”:“http://www.google.co.uk”)

Low-level event format: provenance

dataprov_source	/Users/Chris/NTUSER.DAT
dataprov_type	offset
dataprov_value	274784

Currently identified data provenance

- **offset**, e.g. in a Registry hive, index.dat, $mft
- **sql statement**, e.g. places.sqlite
- **line number**, e.g. setupapi.log

We have a SQLite database containing millions of low-level events

id	min_date_time	max_date_time	evidence	plugin	type	path	dataprov_source	dataprov_type	dataprov_va
0	1300991498.468	1300991498.468	HC-TechCom	MFT	Created	/$MFT	/$MFT	offset	0
1	1300991498.468	1300991498.468	HC-TechCom	MFT	Modified	/$MFT	/$MFT	offset	0
2	1300991498.468	1300991498.468	HC-TechCom	MFT	Entry Modified	/$MFT	/$MFT	offset	0
3	1300991498.468	1300991498.468	HC-TechCom	MFT	Accessed	/$MFT	/$MFT	offset	0
4	1300991498.468	1300991498.468	HC-TechCom	MFT	Created	/$MFTMirr	/$MFT	offset	1024
5	1300991498.468	1300991498.468	HC-TechCom	MFT	Modified	/$MFTMirr	/$MFT	offset	1024
6	1300991498.468	1300991498.468	HC-TechCom	MFT	Entry Modified	/$MFTMirr	/$MFT	offset	1024
7	1300991498.468	1300991498.468	HC-TechCom	MFT	Accessed	/$MFTMirr	/$MFT	offset	1024
8	1300991498.468	1300991498.468	HC-TechCom	MFT	Created	/$LogFile	/$MFT	offset	2048
9	1300991498.468	1300991498.468	HC-TechCom	MFT	Modified	/$LogFile	/$MFT	offset	2048
10	1300991498.468	1300991498.468	HC-TechCom	MFT	Entry Modified	/$LogFile	/$MFT	offset	2048
11	1300991498.468	1300991498.468	HC-TechCom	MFT	Accessed	/$LogFile	/$MFT	offset	2048
12	1300991498.468	1300991498.468	HC-TechCom	MFT	Created	/$Volume	/$MFT	offset	3072
13	1300991498.468	1300991498.468	HC-TechCom	MFT	Modified	/$Volume	/$MFT	offset	3072
14	1300991498.468	1300991498.468	HC-TechCom	MFT	Entry Modified	/$Volume	/$MFT	offset	3072
15	1300991498.468	1300991498.468	HC-TechCom	MFT	Accessed	/$Volume	/$MFT	offset	3072
16	1300991498.468	1300991498.468	HC-TechCom	MFT	Created	/$AttrDef	/$MFT	offset	4096
17	1300991498.468	1300991498.468	HC-TechCom	MFT	Modified	/$AttrDef	/$MFT	offset	4096
18	1300991498.468	1300991498.468	HC-TechCom	MFT	Entry Modified	/$AttrDef	/$MFT	offset	4096
19	1300991498.468	1300991498.468	HC-TechCom	MFT	Accessed	/$AttrDef	/$MFT	offset	4096
20	1300991498.468	1300991498.468	HC-TechCom	MFT	Created	/$Bitmap	/$MFT	offset	6144
21	1300991498.468	1300991498.468	HC-TechCom	MFT	Modified	/$Bitmap	/$MFT	offset	6144
22	1300991498.468	1300991498.468	HC-TechCom	MFT	Entry Modified	/$Bitmap	/$MFT	offset	6144
23	1300991498.468	1300991498.468	HC-TechCom	MFT	Accessed	/$Bitmap	/$MFT	offset	6144
24	1300991498.468	1300991498.468	HC-TechCom	MFT	Created	/$Boot	/$MFT	offset	7168
25	1300991498.468	1300991498.468	HC-TechCom	MFT	Modified	/$Boot	/$MFT	offset	7168

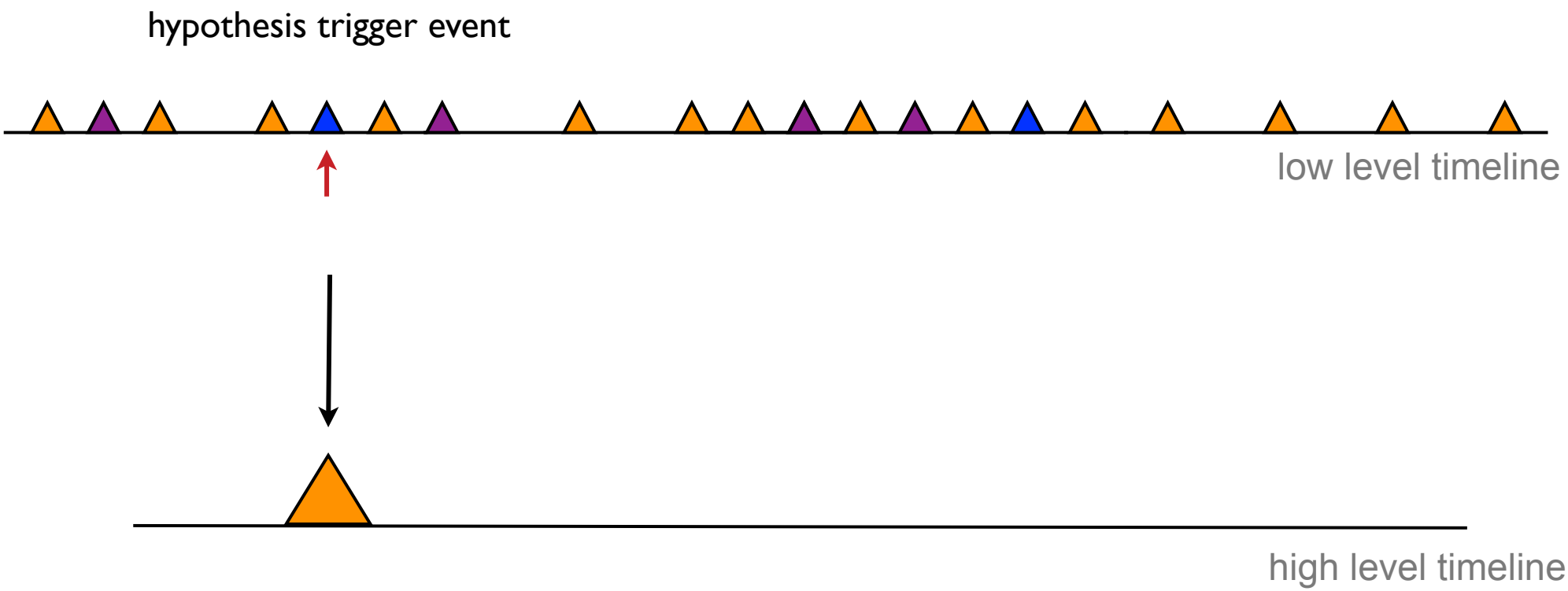
select *, rowid "NAVICAT_ROWID" from "main"."events" limit 0,1000

1

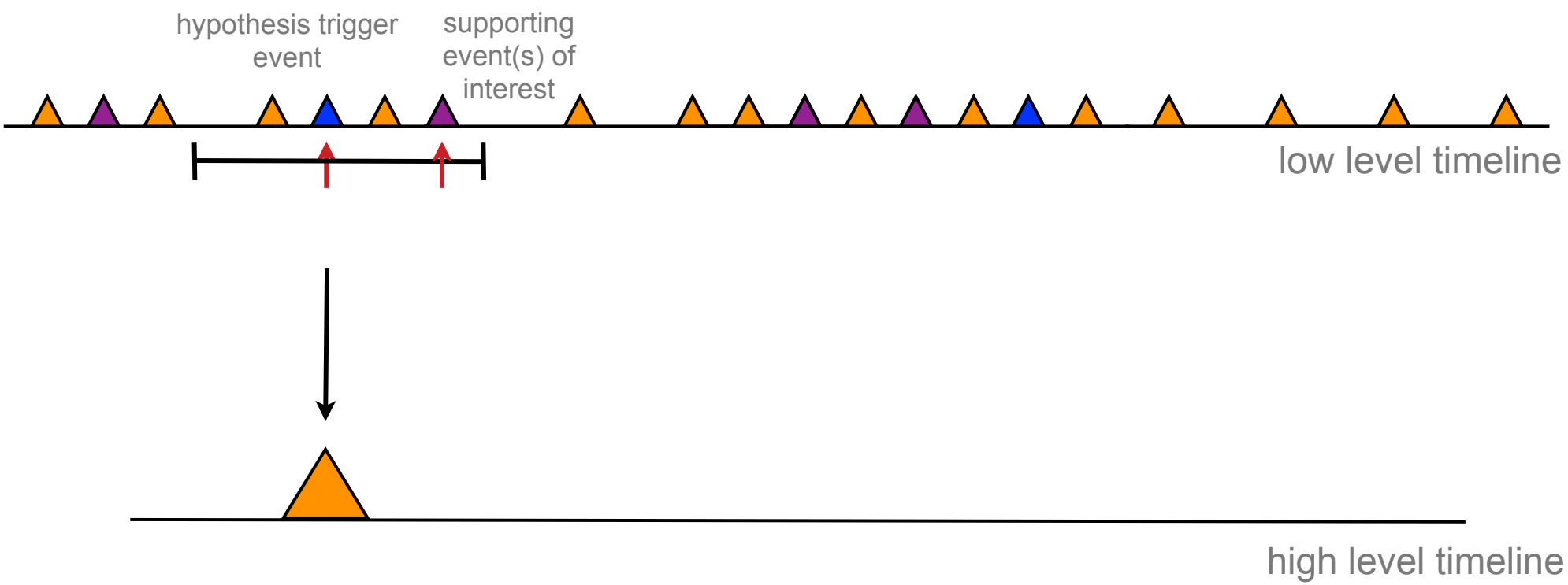
1000 records in page 1

Automated Analysis

Analysis Concept (simple)



Analysis Concept (slightly more complex)



Simple test events

```
flickr_search_test = PyDFT.Core.LowLevelEvent.LowLevelEvent()
flickr_search_test.type = "URL Visit"
flickr_search_test.path = "http://www\.flickr.com/search/\?q=([^&]+)"
```

Events can be directly compared

```
def __eq__(self, other):
    """A low level event is the same as another if all the attributes match"""
    if type(other) != PyDFT.Core.LowLevelEvent.LowLevelEvent:
        return False
    if self.evidence != other.evidence:
        return False
    if self.plugin != other.plugin:
        return False
    if self.event_provenance.source != other.event_provenance.source:
        return False
    if self.event_provenance.type != other.event_provenance.type:
        return False
    if self.event_provenance.value != other.event_provenance.value:
        return False
    if self.date_time_min != other.date_time_min:
        return False
    if self.date_time_max != other.date_time_max:
        return False
    if self.path != other.path:
        return False
    if self.type != other.type:
        return False
    if self.keys != other.keys:
        return False
    return True
```

...but searches are more powerful if you can use regex

```
def Match(self, test_event):
    """Tries to match a test event with the current event and returns true if they match"""
    if not re.search(test_event.evidence, self.evidence):
        return None
    if not re.search(test_event.type, self.type):
        return None
    if not re.search(test_event.plugin, self.plugin):
        return None
    if re.search(test_event.path, self.path) == None:
        return None
    if test_event.event_provenance.source != None:
        if not re.search(test_event.event_provenance.source, self.event_provenance.source):
            return None
    if test_event.event_provenance.type != None:
        if not re.search(test_event.event_provenance.type, self.event_provenance.type):
            return None
    if test_event.event_provenance.value != None:
        if not re.search(test_event.event_provenance.value, self.event_provenance.value):
            return None
    for each_test_key in test_event.keys:
        # if key does not exist...
        if each_test_key not in self.keys:
            return None
        # if key data does not match...
        if not re.search(test_event.keys[each_test_key], self.keys[each_test_key]):
            return None
    else:
        return True
```

Basic Event Matching

```
def AmazonSearches(low_timeline, queue, start_id, end_id):

    test_events_dict = GetAmazonTestEvents()
    trigger_matches_from_low_timeline = low_timeline.FindMatchingEventsinIdRange(start_id,end_id, test_events_dict)

    high_level_timeline = PyDFT.Core.HighLevelTimeline.HighLevelTimeline()

    for each_low_event in trigger_matches_from_low_timeline:
        matched_trigger = each_low_event.MatchAnyTestEvent(test_events_dict)
        if matched_trigger:
            # make high level event
            high_event = PyDFT.Core.HighLevelEvent.HighLevelEvent()
            high_event.AddTime(each_low_event.date_time_min)
            high_event.AddTime(each_low_event.date_time_max)
            high_event.type = "Amazon search"
            high_event.category = "Web"
            high_event.evidence_source = each_low_event.evidence
            high_event.device = each_low_event.evidence

            # get search terms and other detail
            search_term = GetSearchTermFromURL(test_events_dict[matched_trigger].path, each_low_event.path)
            high_event.description = "Amazon search for '%s'" % search_term
            high_event.keys["Search term"] = search_term
            if "Page Title" in each_low_event.keys:
                high_event.keys["Page Title"] = each_low_event.keys["Page Title"]

            # Add reasoning for this high level event
            reasoning = PyDFT.Core.HighLevelEvent.ReasoningArtefact()
            reasoning.id = each_low_event.id
            reasoning.test_event = test_events_dict[matched_trigger]
            reasoning.description = "Amazon search URL found (%s)" % each_low_event.path
            high_event.trigger = reasoning

            # Add the event to the high-level timeline
            high_level_timeline.AddEvent(high_event)

    queue.put(high_level_timeline)
```

More Complex Event Matching

Methods for matching

```
MatchAnyTestEvent(self, dict_of_test_events)


FindMatchingEventsinIdRange(self, start, end, test_events)

FindEventsInSubTimeline(self, event_list, start, end)

FindEventsRelatedToAPath(self, path)
```

YouTube example test events

```
# Construct the test event -- matching url
trigger_test_event = LowLevelEvent.LowLevelEvent()
trigger_test_event.type = "URL Visit"
trigger_test_event.path = "http://[a-zA-Z0-9]*?\.youtube\.com/watch\?v=([^&]+)&?(.*)"


videoplayback_access_test = PyDFT.Core.LowLevelEvent.LowLevelEvent()
videoplayback_access_test.type = "Accessed"
videoplayback_access_test.path = "/Temporary Internet Files/Low/Content.IE5/(.+)/(videoplayback\[[0-9]{1}\])"


videoplayback_modify_test = PyDFT.Core.LowLevelEvent.LowLevelEvent()
videoplayback_modify_test.type = "Modified"
videoplayback_modify_test.path = "/Temporary Internet Files/Low/Content.IE5/(.+)/(videoplayback\[[0-9]{1}\])"

videoplayback_firefox_test = PyDFT.Core.LowLevelEvent.LowLevelEvent()
videoplayback_firefox_test.plugin = "Firefox Cache"
videoplayback_firefox_test.type = "Cached"
videoplayback_firefox_test.keys["url"] = ".*?youtube.com/videoplayback"
```

Patterson, J. & Hargreaves, C. (2011) Automated Identification and Reconstruction of YouTube Video Access, Proceedings from 5th Cybercrime Forensics Education and Training

High-level event format

```
<event>
    <min_date_time>1291573279.718</min_date_time>
    <max_date_time>1291573279.718</max_date_time>
    <evidence_source>CH-Smythe-01</evidence_source>
    <description>Google Search for 'pdf creator'</description>
    <category>Web</category>
    <device>CH-Smythe-01</device>
    <type>Google Search</type>
    <files></files>
    <summary></summary>
    <trigger_evidence_artefact>
        <reasoning_artefact>
            <description>Google search URL found in /Documents and Settings/Alan/Local Set
            <id>42117</id>
            <test_event>
                <low_event>
                    <type>URL Visit</type>
                    <path>http://(.+\.)(google)\.[A-z]{2}.*/(.+)</path>
                </low_event>
            </test_event>
        </reasoning_artefact>
    </trigger_evidence_artefact>
    <key name="URL">http://www.google.co.uk/search?hl=en&source=hp&q=pdf+creator&meta=&aq=
    <key name="Search_Term">pdf creator</key>
    <key name="Browser">IExplorer</key>
</event>
```

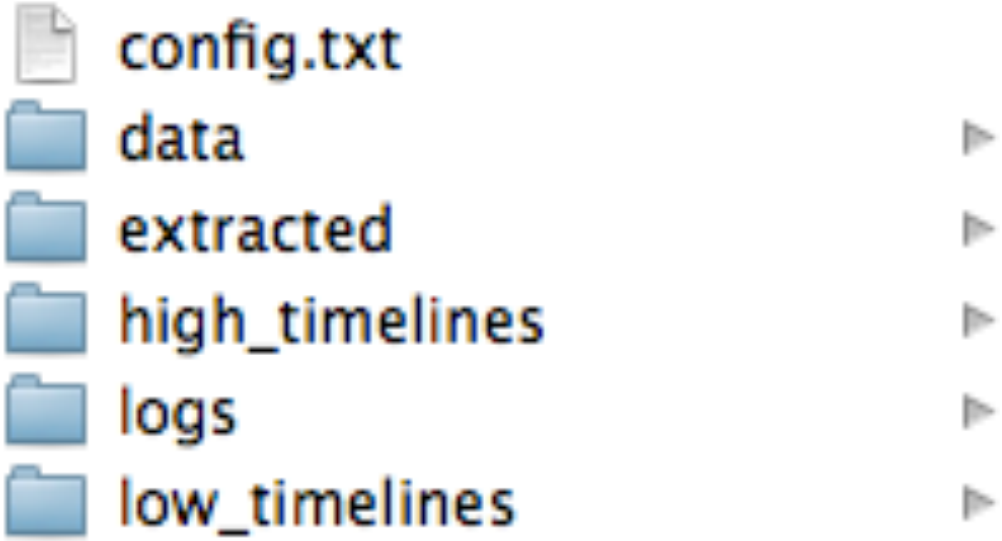
Supporting and contradictory artefacts

```
<supporting_artefacts>
    <reasoning_artefact>
        <description>InstallDate artefact found in Registry</description>
        <id>553204</id>
        <test_event>
            <low_event>
                <plugin>Registry Parser</plugin>
                <path>}/Microsoft/Windows NT/CurrentVersion$</path>
                <key name="InstallDate">.*</key>
            </low_event>
        </test_event>
    </reasoning_artefact>
</supporting_artefacts>
<contradictory_artefacts>
    <reasoning_artefact>
        <description>Windows Folder created not found at similar time</description>
        <id>-1</id>
        <test_event>
            <low_event>
                <plugin>Mounted File System</plugin>
                <type>Created</type>
                <path>^Windows$</path>
            </low_event>
        </test_event>
    </reasoning_artefact>
</contradictory_artefacts>
```

High-level event format

```
<event>
    <min_date_time>1291579906</min_date_time>
    <max_date_time>1291579906</max_date_time>
    <evidence_source>CH-Smythe-01</evidence_source>
    <description>panther.pdf created</description>
    <category>User Activity</category>
    <device>CH-Smythe-01</device>
    <type>PDF created</type>
    <files>
        <file>
            <original_file>/Documents and Settings/Alan/Desktop/panther.pdf</original_file>
            <copied_file>CH-Smythe-01_0000000A.pdf</copied_file>
        </file>
    </files>
    <summary></summary>
    <trigger_evidence_artefact>
        <reasoning_artefact>
            <description>Created time for .pdf file panther.pdf in /Documents and Settings/Alan/Desktop/</des
            <id>329</id>
            <test_event>
                <low_event>
                    <type>Created</type>
                    <path>.+\.pdf$</path>
                </low_event>
            </test_event>
        </reasoning_artefact>
    </trigger_evidence_artefact>
    <key name="File Size">39880</key>
    <key name="File Name">panther.pdf</key>
    <key name="File Path">/Documents and Settings/Alan/Desktop/panther.pdf</key>
</event>
```

Case folder structure



Results

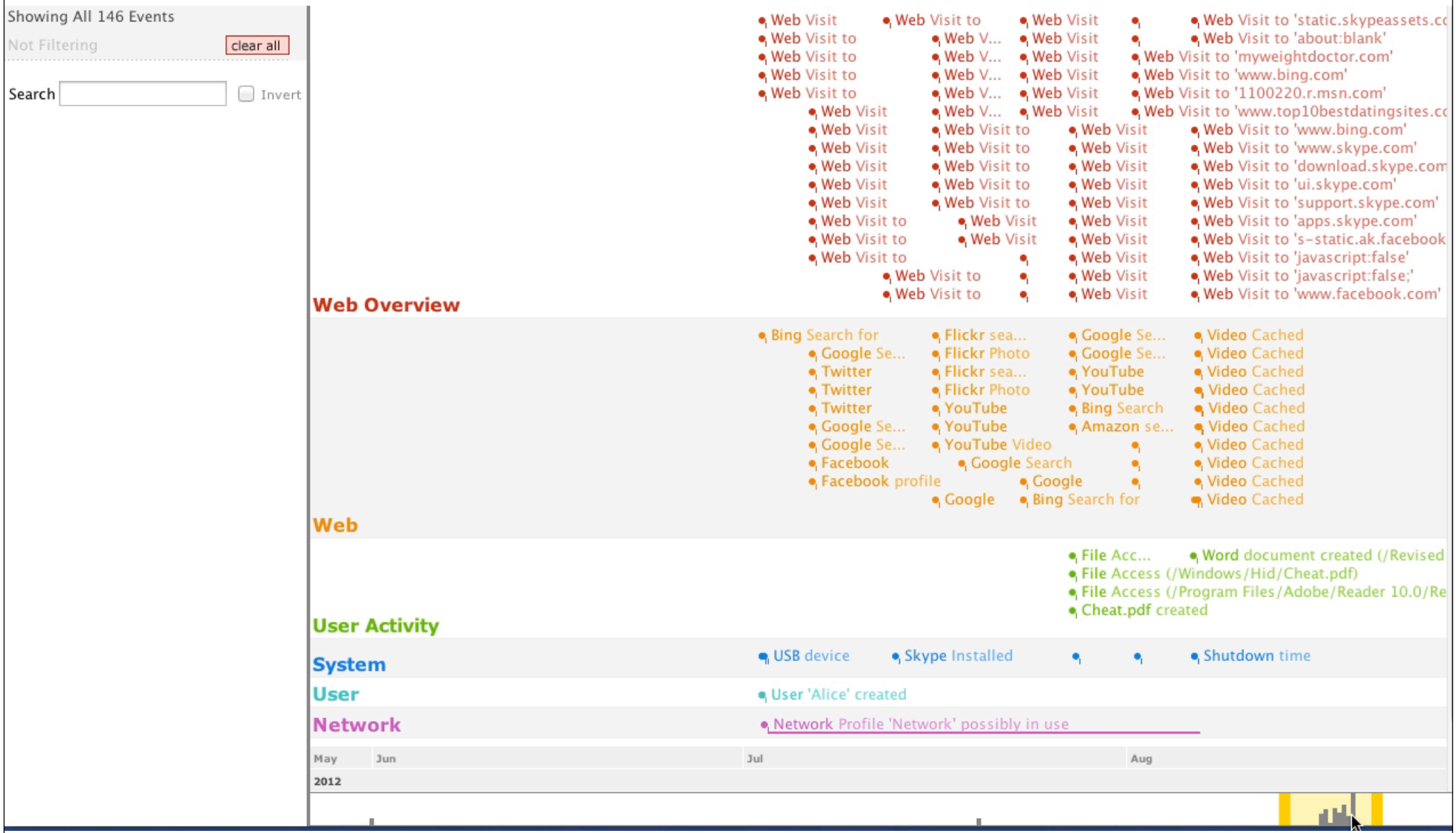
Performance

Table 1
Example times for timeline generation and analysis. The first is from a small, test VM, others are from 'real world' systems.

Volume size	Approx. time system in use	Low-events produced	Time for low generation (hh:mm)
20 GB	2 months	0.6 million	0:15
100 GB	2 years	1.2 million	0:42
250 GB	5 years	1.6 million	1:05

Volume size	Number of analysers	High-events produced	Time for analysis
20 GB	19	666	0:28
100 GB	19	2704	1:10
250 GB	17	3902	1:14

Visualising high-level timelines using Timeflow



https://github.com/FlowingMedia/**TimeFlow**/wiki/

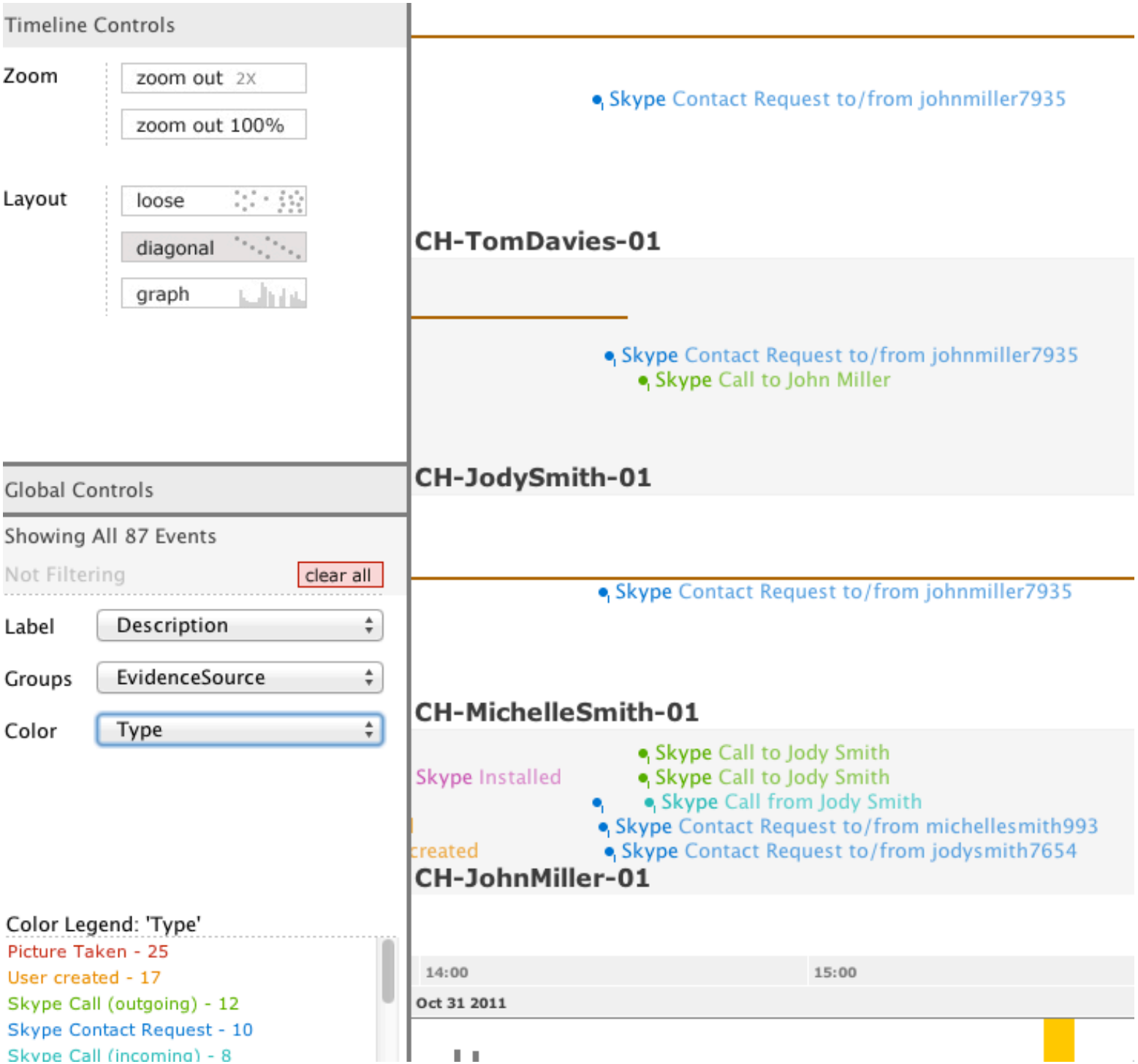
Devices

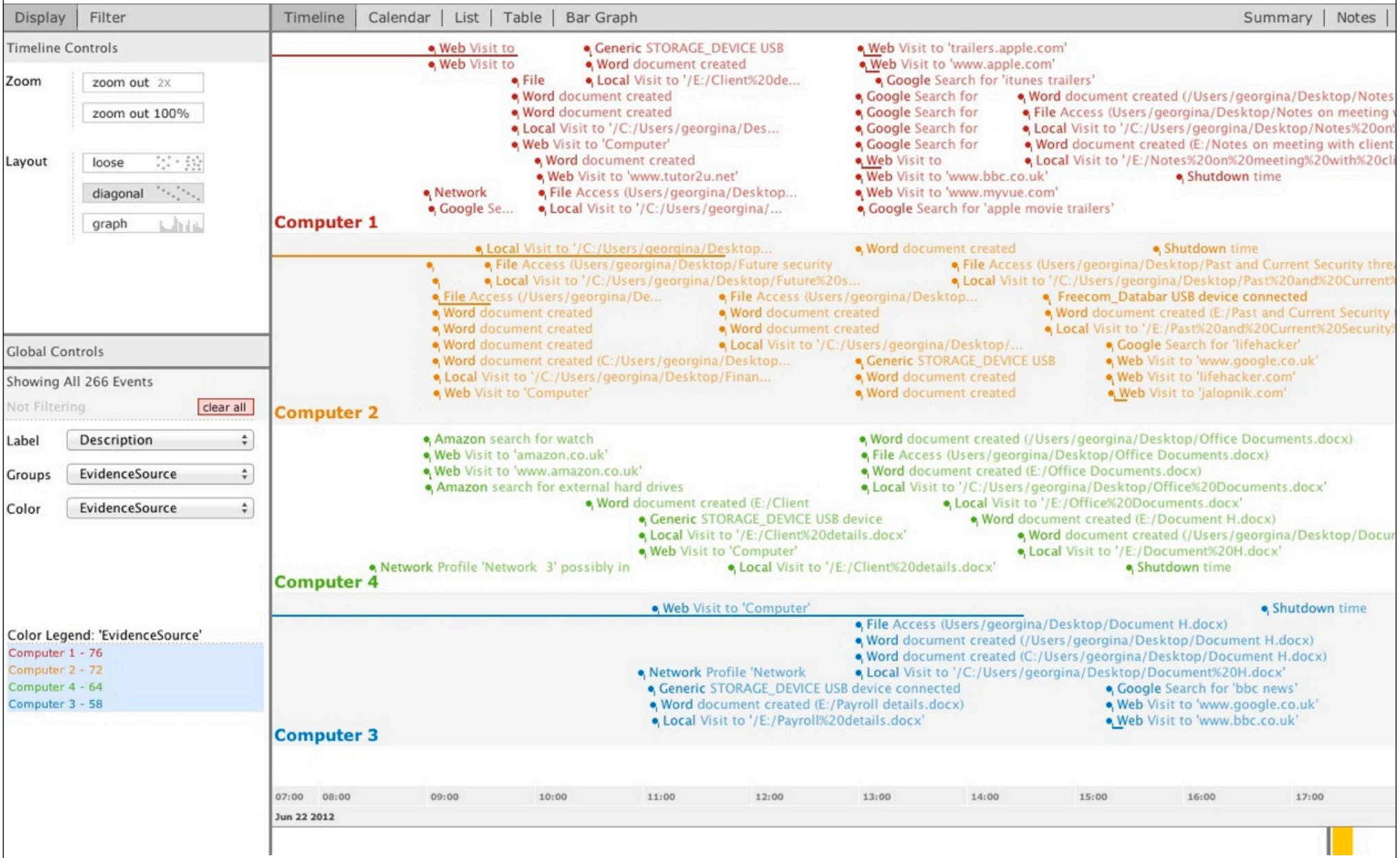
USB device connected (E:/)

User Activity

Word document created (/Users/gordon/Documents/hack-wifi.docx)

Word document created (E:/hack-wifi.docx)


Timeline Controls
Zoom
zoom out 2X
zoom out 100%
Layout
loose
diagonal
graph
Global Controls
Showing All 87 Events
Not Filtering
clear all
Label
Description
Groups
EvidenceSource
Color
Type
Color Legend: 'Type'
Picture Taken - 25
User created - 17
Skype Call (outgoing) - 12
Skype Contact Request - 10
Skype Call (incoming) - 8
Skype Contact Request to/from johnmiller7935
CH-TomDavies-01
Skype Contact Request to/from johnmiller7935
Skype Call to John Miller
CH-JodySmith-01
Skype Contact Request to/from johnmiller7935
CH-MichelleSmith-01
Skype Call to Jody Smith
Skype Installed
Skype Call to Jody Smith
Skype Call from Jody Smith
Skype Contact Request to/from michellesmith993
created
Skype Contact Request to/from jodysmith7654
CH-JohnMiller-01
14:00
15:00
Oct 31 2011


Display
Filter
Timeline
Calendar
List
Table
Bar Graph
Summary
Notes
Timeline Controls
Zoom
zoom out 2x
zoom out 100%
Layout
loose
diagonal
graph
Global Controls
Showing All 266 Events
Not Filtering
clear all
Label
Description
Groups
EvidenceSource
Color
EvidenceSource
Color Legend: 'EvidenceSource'
Computer 1 - 76
Computer 2 - 72
Computer 4 - 64
Computer 3 - 58
Web Visit to
Web Visit to
Generic STORAGE_DEVICE USB
Word document created
File
Local Visit to '/E:/Client%20de...
Word document created
Word document created
Local Visit to '/C:/Users/georgina/Des...
Web Visit to 'Computer'
Word document created
Web Visit to 'www.tutor2u.net'
Network
File Access (Users/georgina/Desktop...
Google Se...
Local Visit to '/C:/Users/georgina/...
Web Visit to 'trailers.apple.com'
Web Visit to 'www.apple.com'
Google Search for 'itunes trailers'
Google Search for
Google Search for
Google Search for
Google Search for
Web Visit to
Web Visit to 'www.bbc.co.uk'
Web Visit to 'www.myvue.com'
Google Search for 'apple movie trailers'
Word document created (/Users/georgina/Desktop/Notes
File Access (Users/georgina/Desktop/Notes on meeting
Local Visit to '/C:/Users/georgina/Desktop/Notes%20on
Word document created (E:/Notes on meeting with client
Local Visit to '/E:/Notes%20on%20meeting%20with%20cli
Shutdown time
Computer 1
Local Visit to '/C:/Users/georgina/Desktop...
Word document created
Shutdown time
File Access (Users/georgina/Desktop/Future security
Local Visit to '/C:/Users/georgina/Desktop/Future%20s...
File Access (Users/georgina/Desktop/Past and Current Security thre
Local Visit to '/C:/Users/georgina/Desktop/Past%20and%20Current
File Access (/Users/georgina/De...
File Access (Users/georgina/Desktop...
Freecom_Databar USB device connected
Word document created
Word document created
Word document created (E:/Past and Current Security
Word document created
Word document created
Local Visit to '/E:/Past%20and%20Current%20Security
Word document created
Local Visit to '/C:/Users/georgina/Desktop/...
Google Search for 'lifehacker'
Word document created (C:/Users/georgina/Desktop...
Generic STORAGE_DEVICE USB
Web Visit to 'www.google.co.uk'
Local Visit to '/C:/Users/georgina/Desktop/Finan...
Word document created
Web Visit to 'lifehacker.com'
Web Visit to 'Computer'
Word document created
Web Visit to 'jalopnik.com'
Computer 2
Amazon search for watch
Web Visit to 'amazon.co.uk'
Web Visit to 'www.amazon.co.uk'
Amazon search for external hard drives
Word document created (E:/Client
Generic STORAGE_DEVICE USB device
Local Visit to '/E:/Client%20details.docx'
Web Visit to 'Computer'
Network Profile 'Network 3' possibly in
Local Visit to '/E:/Client%20details.docx'
Word document created (/Users/georgina/Desktop/Office Documents.docx)
File Access (Users/georgina/Desktop/Office Documents.docx)
Word document created (E:/Office Documents.docx)
Local Visit to '/C:/Users/georgina/Desktop/Office%20Documents.docx'
Local Visit to '/E:/Office%20Documents.docx'
Word document created (E:/Document H.docx)
Word document created (/Users/georgina/Desktop/Docu
Local Visit to '/E:/Document%20H.docx'
Shutdown time
Computer 4
Web Visit to 'Computer'
Shutdown time
File Access (Users/georgina/Desktop/Document H.docx)
Word document created (/Users/georgina/Desktop/Document H.docx)
Word document created (C:/Users/georgina/Desktop/Document H.docx)
Network Profile 'Network
Local Visit to '/C:/Users/georgina/Desktop/Document%20H.docx'
Generic STORAGE_DEVICE USB device connected
Google Search for 'bbc news'
Word document created (E:/Payroll details.docx)
Web Visit to 'www.google.co.uk'
Local Visit to '/E:/Payroll%20details.docx'
Web Visit to 'www.bbc.co.uk'
Computer 3
07:00
08:00
09:00
10:00
11:00
12:00
13:00
14:00
15:00
16:00
17:00
Jun 22 2012

Visualising high-level timelines using d3.js (work in progress)

d3.js used to show high and supporting low-level events

1385	Sat Mar 26 2011 08:14:19 GMT-0400 (EDT)	Sat Mar 26 2011 08:14:19 GMT-0400 (EDT)	HC-TechCom	Web Visit to 'uk.msn.com'	Web Overview	HC-TechCom	Web Visit
1464	Sat Mar 26 2011 08:14:45 GMT-0400 (EDT)	Sat Mar 26 2011 08:15:27 GMT-0400 (EDT)	HC-TechCom	Web Visit to 'res:'	Web Overview	HC-TechCom	Web Visit
1462	Sat Mar 26 2011 08:15:00 GMT-0400 (EDT)	Sat Mar 26 2011 08:15:00 GMT-0400 (EDT)	HC-TechCom	Web Visit to 'track.searchignite.com'	Web Overview	HC-TechCom	Web Visit
1446	Sat Mar 26 2011 08:15:04 GMT-0400 (EDT)	Sat Mar 26 2011 08:15:22 GMT-0400 (EDT)	HC-TechCom	Web Visit to 'www.apple.com'	Web Overview	HC-TechCom	Web Visit
1367	Sat Mar 26 2011 08:15:24 GMT-0400 (EDT)	Sat Mar 26 2011 08:15:24 GMT-0400 (EDT)	HC-TechCom	Google Search for 'laptops'	Web	HC-TechCom	Google Search
1445	Sat Mar 26 2011 08:15:24 GMT-0400 (EDT)	Sat Mar 26 2011 08:15:27 GMT-0400 (EDT)	HC-TechCom	Web Visit to 'www.google.co.uk'	Web Overview	HC-TechCom	Web Visit
1361	Sat Mar 26 2011 08:15:27 GMT-0400 (EDT)	Sat Mar 26 2011 08:15:27 GMT-0400 (EDT)	HC-TechCom	Google Search for 'laptops'	Web	HC-TechCom	Google Search
1447	Sat Mar 26 2011 08:15:30 GMT-0400 (EDT)	Sat Mar 26 2011 08:15:38 GMT-0400 (EDT)	HC-TechCom	Web Visit to 'news.idg.no'	Web Overview	HC-TechCom	Web Visit
1467	Sat Mar 26 2011 08:19:51 GMT-0400 (EDT)	Sat Mar 26 2011 08:19:51 GMT-0400 (EDT)	HC-TechCom	Shutdown time	System	HC-TechCom	Shutdown time

High Level Event Details

id: 1467
min_date_time: Sat Mar 26 2011 08:19:51 GMT-0400 (EDT)
max_date_time: Sat Mar 26 2011 08:19:51 GMT-0400 (EDT)
evidence_source: HC-TechCom
description: Shutdown time
category: System
device: HC-TechCom
type: Shutdown time
summary:
keys(0):
files(0):
supporting(1):
- Shutdown time found in /CMI-CreateHive{3D971F19-49AB-4000-8D39-A6D9C673D809}/Microsoft/Windows/CurrentVersion/Reliability/shutdown: 397081
Last Updated/Reliability/shutdown$

contradictory(0):

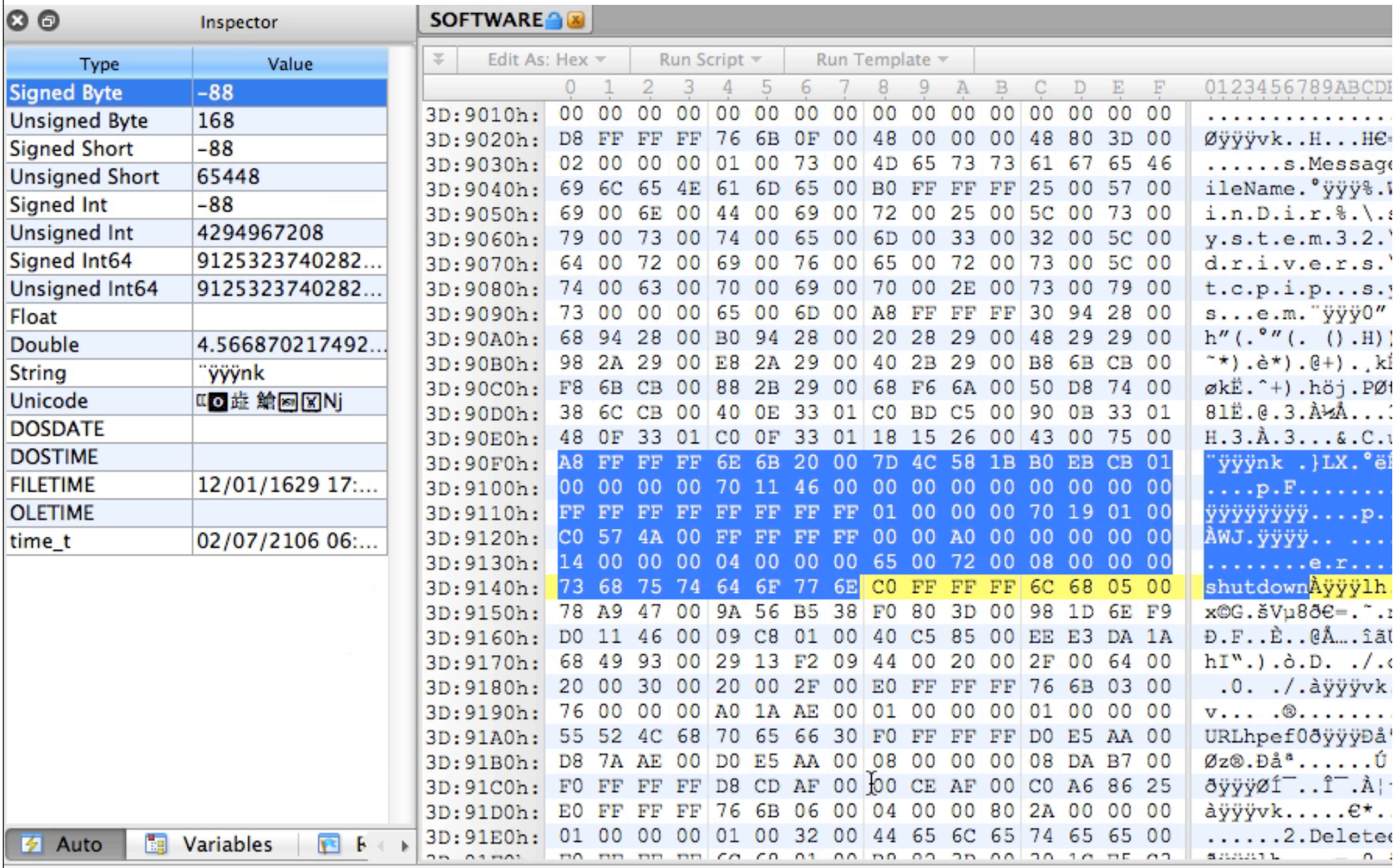
Low Level Event Details

id: 397081
min_date_time: Sat Mar 26 2011 08:19:51 GMT-0400 (EDT)
max_date_time: Sat Mar 26 2011 08:19:51 GMT-0400 (EDT)
evidence: HC-TechCom
plugin: Registry Parser
type: Last Updated
path: /CMI-CreateHive{3D971F19-49AB-4000-8D39-A6D9C673D809}/Microsoft/Windows/CurrentVersion/Reliability/shutdown

dataprov_source: /Windows/System32/config/SOFTWARE
dataprov_type: offset
dataprov_value: 4034800

Keys:
ReasonCode ff000500
type REG_DWORD

Low-event provides link to raw data



Can link to files associated with the event

75	Fri Jul 27 2012 16:45:11 GMT-0400 (EDT)	Fri Jul 27 2012 16:45:12 GMT-0400 (EDT)	JP-Alice_Dylan	Web Visit to '127.0.0.1:49180'	Web Overview	JP-Alice_Dylan	Web Visit
79	Fri Jul 27 2012 16:45:12 GMT-0400 (EDT)	Fri Jul 27 2012 16:45:12 GMT-0400 (EDT)	JP-Alice_Dylan	Web Visit to '127.0.0.1'	Web Overview	JP-Alice_Dylan	Web Visit
20	Fri Jul 27 2012 16:50:36 GMT-0400 (EDT)	Fri Jul 27 2012 16:51:11 GMT-0400 (EDT)	JP-Alice_Dylan	File Access (/Users/Alice/Desktop/Cheat.pdf)	User Activity	JP-Alice_Dylan	File Access
22	Fri Jul 27 2012 16:50:36 GMT-0400 (EDT)	Fri Jul 27 2012 16:53:12 GMT-0400 (EDT)	JP-Alice_Dylan	File Access (/Windows/Hid/Cheat.pdf)	User Activity	JP-Alice_Dylan	File Access
80	Fri Jul 27 2012 16:50:36 GMT-0400 (EDT)	Fri Jul 27 2012 16:50:36 GMT-0400 (EDT)	JP-Alice_Dylan	Web Visit to 'Computer'	Web Overview	JP-Alice_Dylan	Web Visit
21	Fri Jul 27 2012 16:50:46 GMT-0400 (EDT)	Fri Jul 27 2012 16:51:11 GMT-0400 (EDT)	JP-Alice_Dylan	File Access (/Program Files/Adobe/Reader 10.0/Reader/Legal/ENU/license.html)	User Activity	JP-Alice_Dylan	File Access
11	Fri Jul 27 2012 16:52:56 GMT-0400 (EDT)	Fri Jul 27 2012 16:52:56 GMT-0400 (EDT)	JP-Alice_Dylan	Cheat.pdf created	User Activity	JP-Alice_Dylan	PDF created
62	Fri Jul 27 2012 16:55:01 GMT-0400 (EDT)	Fri Jul 27 2012 16:55:01 GMT-0400 (EDT)	JP-Alice_Dylan	Google Search for 'how to kill your husband'	Web	JP-Alice_Dylan	Google Search
	Fri Jul 27 2012 16:55:01 GMT-0400	Fri Jul 27 2012 16:55:37 GMT-0400	JP-			JP-	

High Level Event Details

id: 22
min_date_time: Fri Jul 27 2012 16:50:36 GMT-0400 (EDT)
max_date_time: Fri Jul 27 2012 16:53:12 GMT-0400 (EDT)
evidence_source: JP-Alice_Dylan
description: File Access (/Windows/Hid/Cheat.pdf)
category: User Activity
device: JP-Alice_Dylan
type: File Access
summary:
keys(3):
- Drive_Letter:C:/
- Extension:.pdf
- Filename:Cheat.pdf

files(1):
- Windows/Hid/Cheat.pdf:
JP-Alice_Dylan_00000012.pdf

supporting(5):
- Link file created in Recent Folder

localhost:8000/data/JP-Alice_Dylan_00000012.pdf

Low Level Event Details

id: 225114
min_date_time: Fri Jul 27 2012 16:53:12 GMT-0400 (EDT)
max_date_time: Fri Jul 27 2012 16:53:12 GMT-0400 (EDT)
evidence: JP-Alice_Dylan
plugin: IExplorer Parser
type: URL Visit
path: file:///C:/Windows/Hid/Cheat.pdf

dataprov_source: /Users/Alice/AppData/Local/Microsoft/Windows/History/History.IE5/MSHist012012072720120728/index.dat
dataprov_type: offset
dataprov_value: 22016

Keys:
URL file:///C:/Windows/Hid/Cheat.pdf
Index_Type Daily
User Alice

Can show low-level events that occurred at a similar time

116	Fri Jul 27 2012 16:44:39 GMT-0400 (EDT)	Fri Jul 27 2012 16:44:45 GMT-0400 (EDT)	JP-Alice_Dylan	Web Visit to 'www.google.com'	Web Overview	JP-Alice_Dylan	Web Visit
117	Fri Jul 27 2012 16:44:46 GMT-0400 (EDT)	Fri Jul 27 2012 16:50:24 GMT-0400 (EDT)	JP-Alice_Dylan	Web Visit to 'get.adobe.com'	Web Overview	JP-Alice_Dylan	Web Visit
118	Fri Jul 27 2012 16:44:53 GMT-0400 (EDT)	Fri Jul 27 2012 16:44:53 GMT-0400 (EDT)	JP-Alice_Dylan	Web Visit to 'aihdownload.adobe.com'	Web Overview	JP-Alice_Dylan	Web Visit
75	Fri Jul 27 2012 16:45:11 GMT-0400 (EDT)	Fri Jul 27 2012 16:45:12 GMT-0400 (EDT)	JP-Alice_Dylan	Web Visit to '127.0.0.1:49180'	Web Overview	JP-Alice_Dylan	Web Visit
79	Fri Jul 27 2012 16:45:12 GMT-0400 (EDT)	Fri Jul 27 2012 16:45:12 GMT-0400 (EDT)	JP-Alice_Dylan	Web Visit to '127.0.0.1'	Web Overview	JP-Alice_Dylan	Web Visit
20	Fri Jul 27 2012 16:50:36 GMT-0400 (EDT)	Fri Jul 27 2012 16:51:11 GMT-0400 (EDT)	JP-Alice_Dylan	File Access (/Users/Alice/Desktop/Cheat.pdf)	User Activity	JP-Alice_Dylan	File Access
22	Fri Jul 27 2012 16:50:36 GMT-0400 (EDT)	Fri Jul 27 2012 16:53:12 GMT-0400 (EDT)	JP-Alice_Dylan	File Access (/Windows/Hid/Cheat.pdf)	User Activity	JP-Alice_Dylan	File Access
80	Fri Jul 27 2012 16:50:36 GMT-0400 (EDT)	Fri Jul 27 2012 16:50:36 GMT-0400 (EDT)	JP-Alice_Dylan	Web Visit to 'Computer'	Web Overview	JP-Alice_Dylan	Web Visit

files(1):
- Windows/Hid/Cheat.pdf:
JP-Alice_Dylan_00000012.pdf

supporting(5):
- Link file created in Recent Folder
(/Users/Alice/AppData/Roaming/Microsoft/Windows/Recent/Hid.lnk):
44932
Mounted File SystemlMFT Created
/Users/(.*?)/AppData/Roaming/Microsoft/Windows/Recent/((.*?)\.lnk)

- Recent from Index.dat (file:///C:/Windows/Hid/Cheat.pdf):
225114
IExplorer Parser URL Visit Windows/Hid/Cheat.pdf$

- Recent from Index.dat (file:///C:/Windows/Hid/Cheat.pdf):
225094
IExplorer Parser URL Visit file:///([A-z]{1}:/)(.+/(.+(\.[A-z]{3,4})))$

- Recent from Index.dat (file:///C:/Windows/Hid/Cheat.pdf):
225114
IExplorer Parser URL Visit file:///([A-z]{1}:/)(.+/(.+(\.[A-z]{3,4})))$

NT/CurrentVersion/Schedule/TaskCache/Tree/Microsoft/Windows Defender/MP Scheduled Scan","/Windows/System32/config/SOFTWARE","offset","11608096","Index=03000000","type=REG_DWORD","Id={E411FF2B-B998-4740-817F-643AC040E78C}",

"4436","1343422229.717599","1343422229.717599","JP-Alice_Dylan","MFT","Created","/Windows/System32/LogFiles/Scm/e411ff2b-b998-4740-817f-643ac040e78c","/$MFT","offset","1149952","IsDirectory=False","FileSize=0","MFT_record_number=1123","InUse=True",

"4437","1343422229.717599","1343422229.717599","JP-Alice_Dylan","MFT","Modified","/Windows/System32/LogFiles/Scm/e411ff2b-b998-4740-817f-643ac040e78c","/$MFT","offset","1149952","IsDirectory=False","FileSize=0","MFT_record_number=1123","InUse=True",

"4438","1343422229.717599","1343422229.717599","JP-Alice_Dylan","MFT","Entry Modified","/Windows/System32/LogFiles/Scm/e411ff2b-b998-4740-817f-643ac040e78c","/$MFT","offset","1149952","IsDirectory=False","FileSize=0","MFT_record_number=1123","InUse=True",

"4439","1343422229.717599","1343422229.717599","JP-Alice_Dylan","MFT","Accessed","/Windows/System32/LogFiles/Scm/e411ff2b-b998-4740-817f-643ac040e78c","/$MFT","offset","1149952","IsDirectory=False","FileSize=0","MFT_record_number=1123","InUse=True",

"65312","1343422231.948403","1343422231.948403","JP-Alice_Dylan","MFT","Modified","/Windows/Prefetch/AUDIODG.EXE-BDFD3029.pf","/$MFT","offset","16741376","IsDirectory=False","FileSize=0","MFT_record_number=16349","InUse=True",

Evaluation (1)

- Demonstrated as a feasible approach
- Provenance can be preserved
- Performance-wise ok, and can be improved
- Implementation:
  - Gaps in extractor scope (notably evtx)
  - Supporting and contradictory should be automatically added
  - Analyser scripts need some simplification

Evaluation (2)

- High-level event format is only loosely evaluated with useful examples
- Taxonomy of event types and categories

Future Work

- More extractors including importing from other tools
- More complex analysers
- Testing
- Parallel processing
- Cross-drive analysis
- Evaluation of high-level and low-level timelines
- Visualisations

Questions?

Dr Chris Hargreaves
Lecturer
Centre for Forensic Computing
Cranfield University
Defence Academy of the UK
Shrivenham, UK

c.j.hargreaves@cranfield.ac.uk

Jony Patterson
Research Fellow
Centre for Forensic Computing
Cranfield University
Defence Academy of the UK
Shrivenham, UK

j.patterson@cranfield.ac.uk