Automated Cyber-Readiness Evaluation (ACE)

Rotem Guttman

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

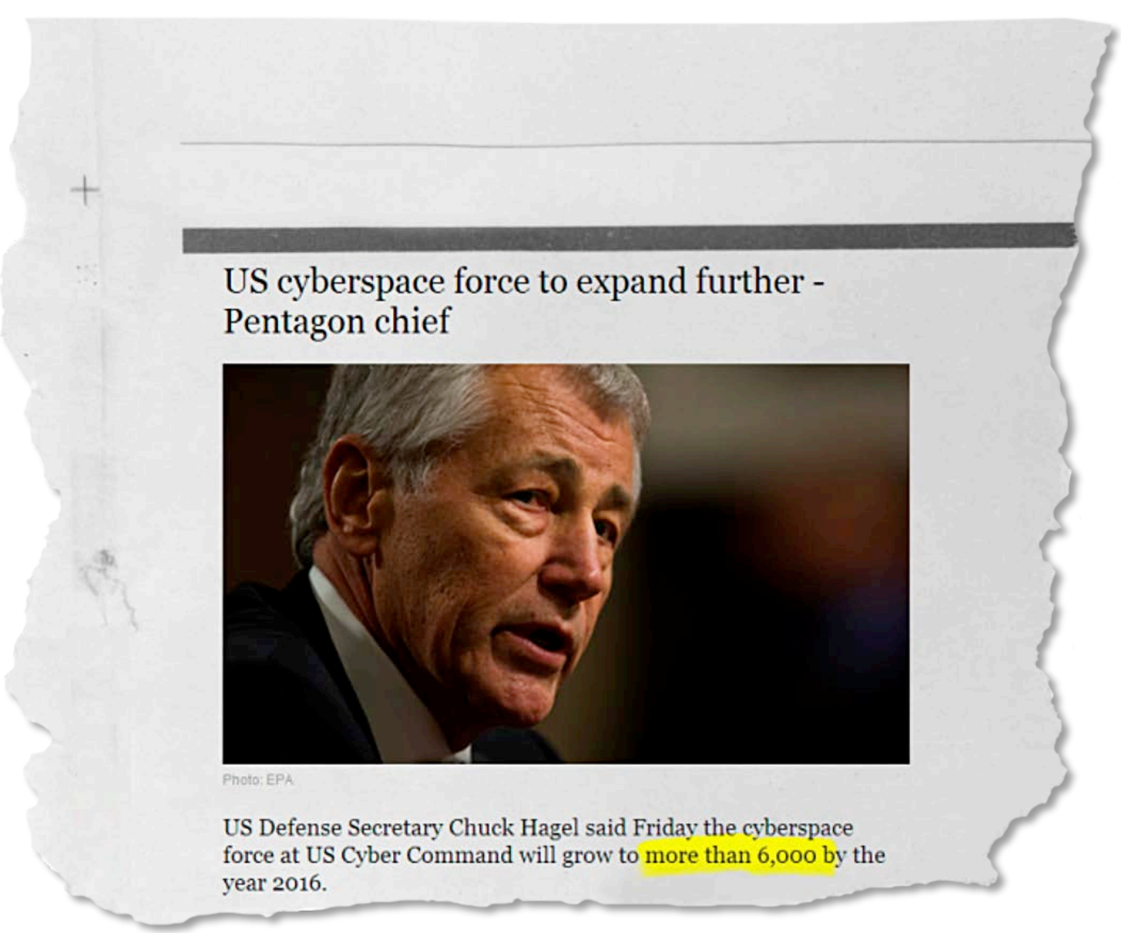
This material is based upon work funded and supported by the Department of Defense under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the United States Department of Defense.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN “AS-IS” BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

DM-0002758

Core DoD Challenge Problem



US cyberspace force to expand further - Pentagon chief

Photo: EPA

US Defense Secretary Chuck Hagel said Friday the cyberspace force at US Cyber Command will grow to more than 6,000 by the year 2016.

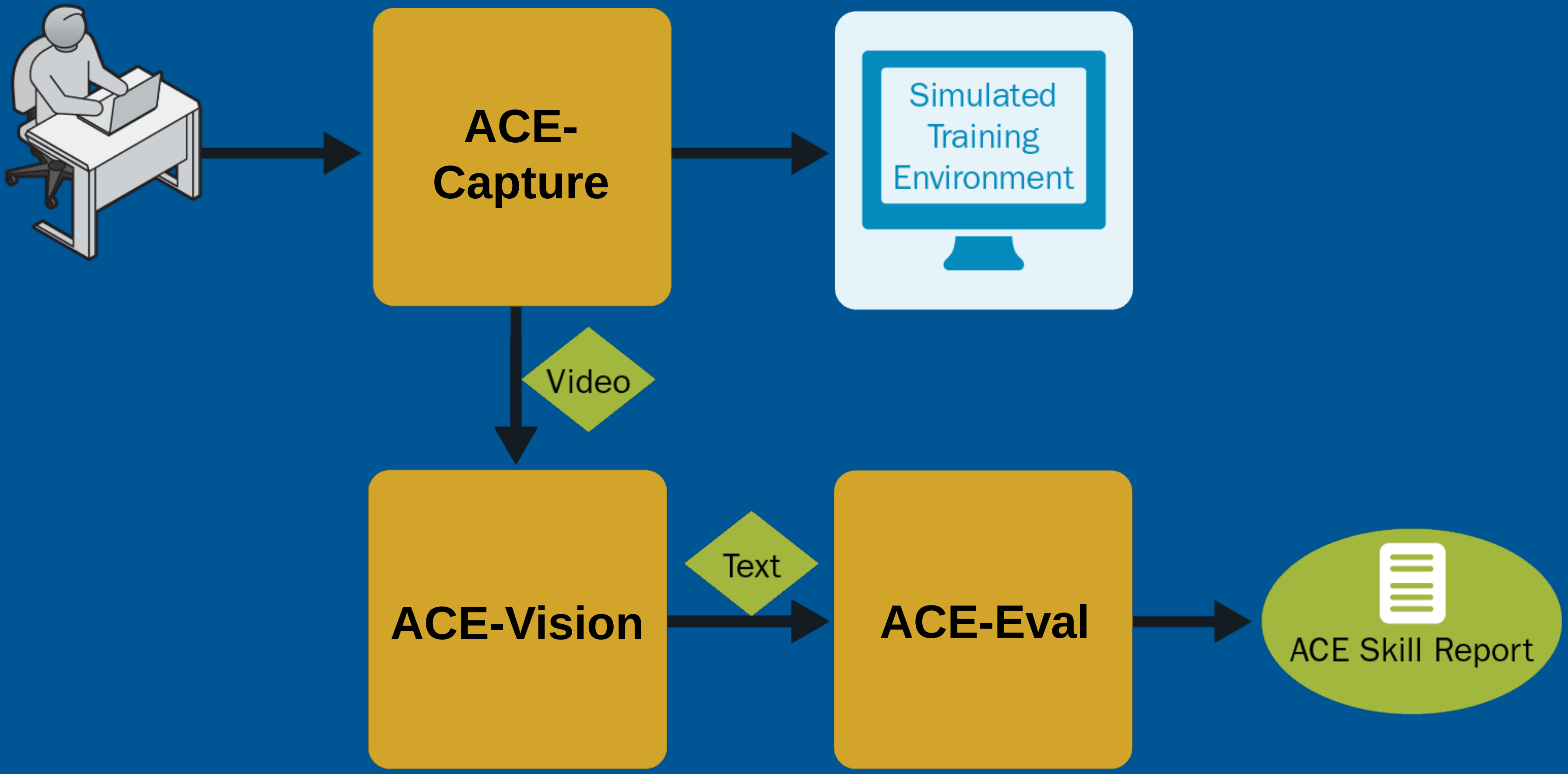
Evaluating Mission-Readiness for Cyber Operators

- **Scalable**
- **Objective**
- **Reliable**
- **Valid**

ACE Philosophy

- **Train as you fight?**
- **Evaluate as you fight!**
  - Place cyber operators in familiar environment
  - Task cyber operators with realistic mission
  - Understand actions taken within scenario
  - Verifiably asses mission-readiness based on actions taken
- **Benefits**
  - Automated Analysis
  - Specific deficiencies isolated
  - Automated remediation plans
  - Recording available for future review

ACE Architecture Overview



Role Choice

Joint Cyberspace Training &

Certification Standards (JCT&CS)

Forensic Analyst

- 2 Hours
- Existing DoD Standard
- Self-Contained

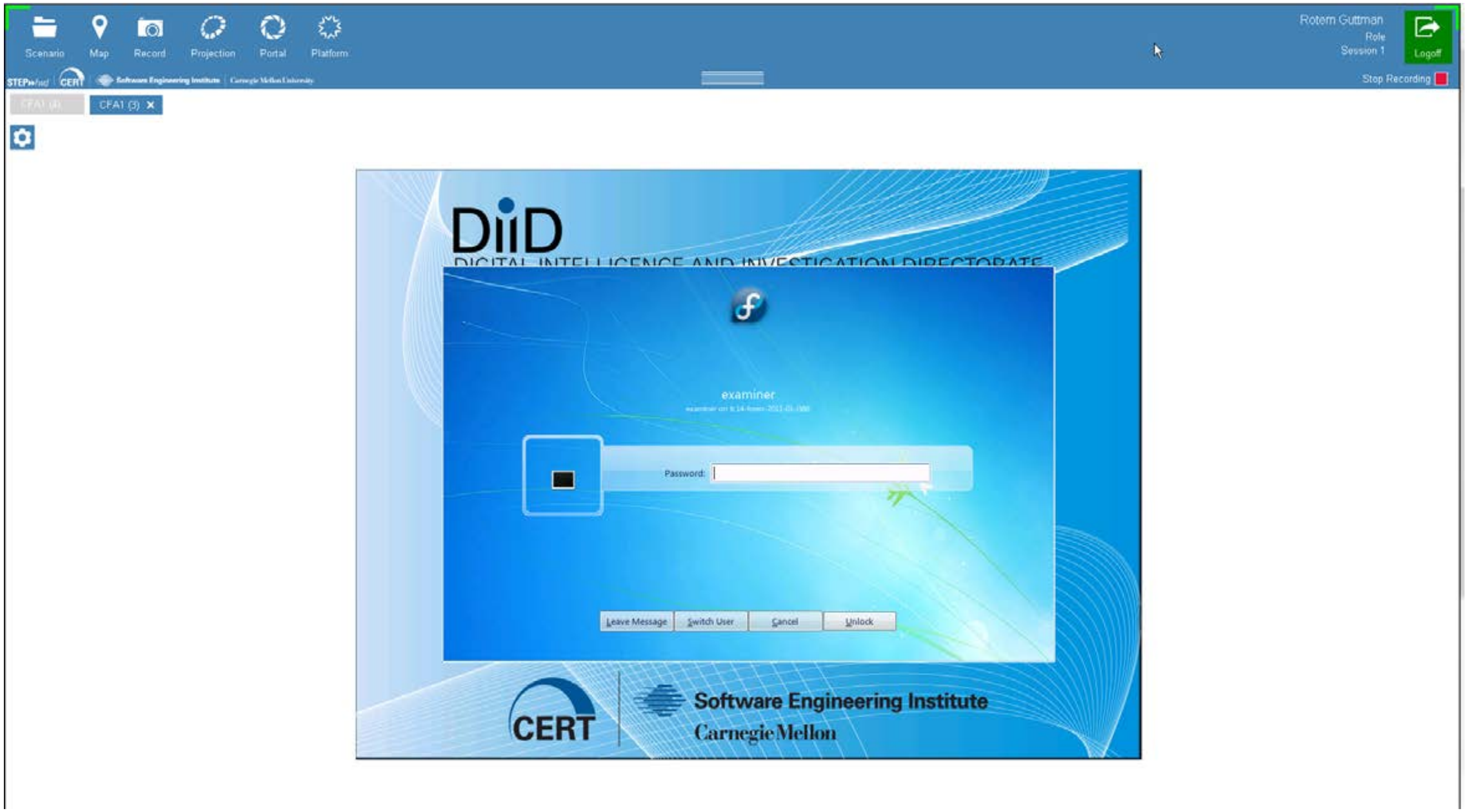
Scenario Development

Scenario I & II Details

- **Missing Person**
  - Foul Play Suspected
- **Classified* Documents Exfiltrated**
  - Computer Drive Image
  - Multiple Layers of Story
    - APT1
    - USB
    - Personal Email

***Fabricated Documents**
(Not actual classified data)

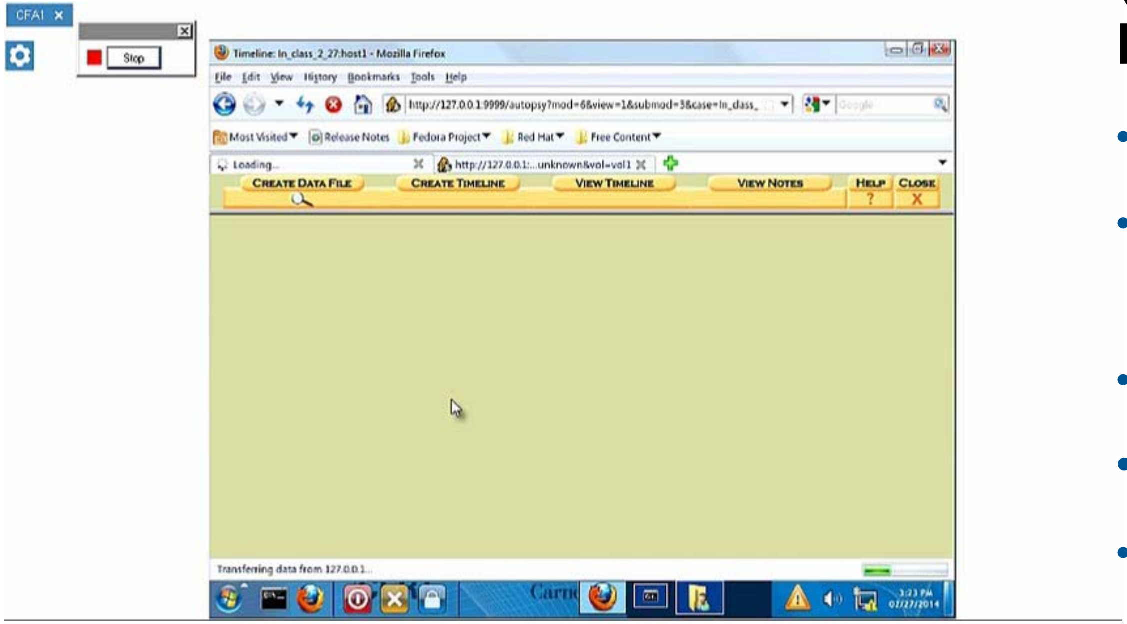
Data Collection Capability



Password:

- **Background Data Collection**
- **Restricted to Environment**
- **Scalable**

Data Collection


CFA1 ×
Stop
Timeline: In_class_2_27:host1 - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://127.0.0.1:9999/autopsy?mod=6&view=1&submod=3&case=In_class_
Google
Most Visited Release Notes Fedora Project Red Hat Free Content
Loading...
http://127.0.0.1:...unknown&vol=vol1
CREATE DATA FILE
CREATE TIMELINE
VIEW TIMELINE
VIEW NOTES
HELP ?
CLOSE X
Transferring data from 127.0.0.1...
3:23 PM
02/27/2014

Multiple Sources (Increase Dataset Robustness)

- CERT Staff
- CMU Graduate Students
- DoD Personnel
- Multiple Collections
- NCFTA Personnel

ACE-Vision

Primary Collaborator:
Professor Yaser Sheik

CMU Robotics Institute, Graphics Lab

Custom Detection System

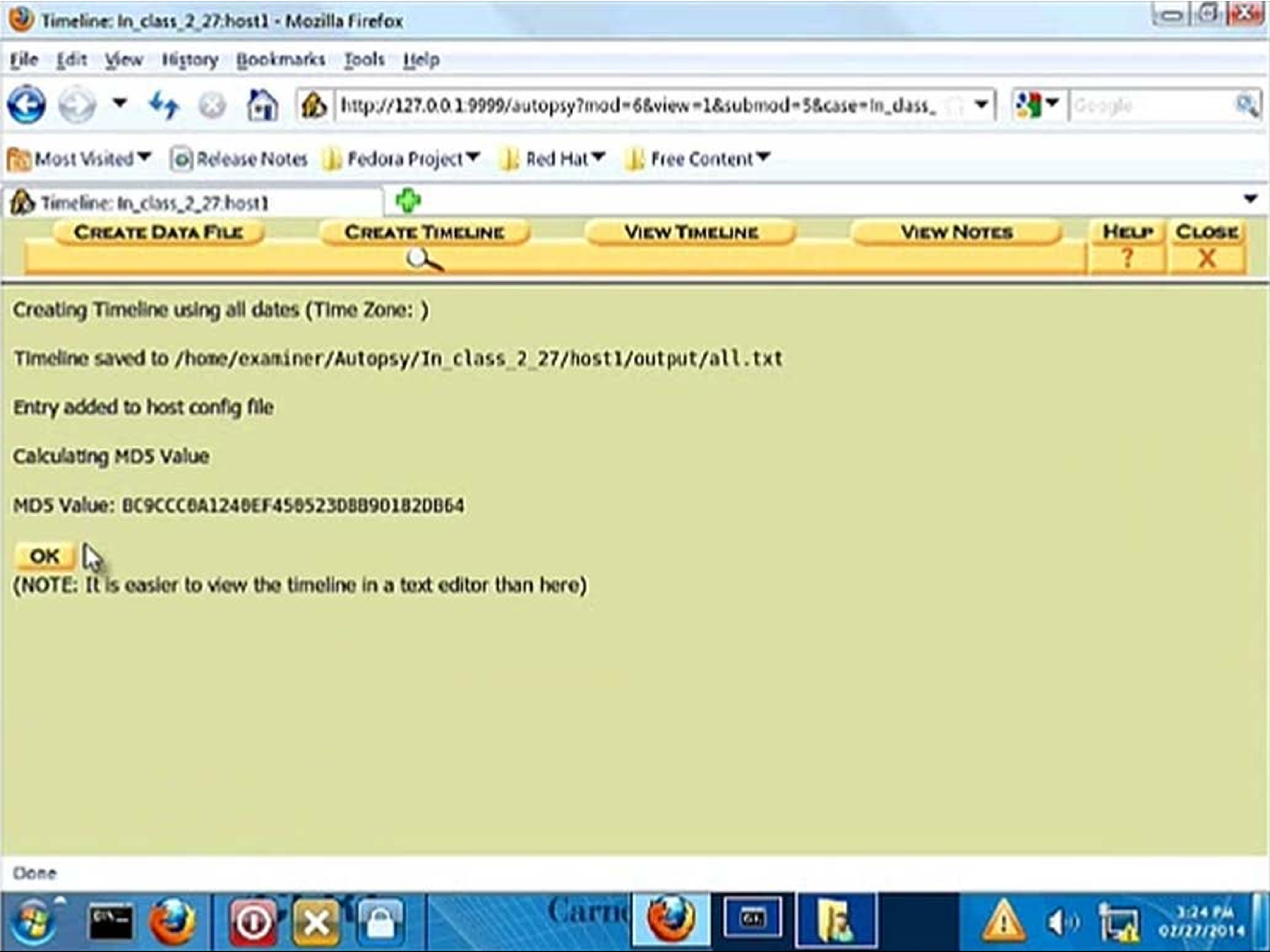
Designed for massive parallelization

Optimized for use case:

- Maximize pre-process capability
- Minimize duplicate calculations

- Original: O(nN)
  - Infeasable for our problem set.
- Optimized: O(NlogN) time.
  - Implemented on GPU array.

Note: Our data set uses high resolution images and so n >> logN


Timeline: In_class_2_27:host1 - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://127.0.0.1:9999/autopsy?mod=6&view=1&submod=5&case=In_class_
Google
Most Visited
Release Notes
Fedora Project
Red Hat
Free Content
Timeline: In_class_2_27:host1
CREATE DATA FILE
CREATE TIMELINE
VIEW TIMELINE
VIEW NOTES
HELP
?
CLOSE
X
OK
Done
3:24 PM
02/27/2014

Creating Timeline using all dates (Time Zone:)

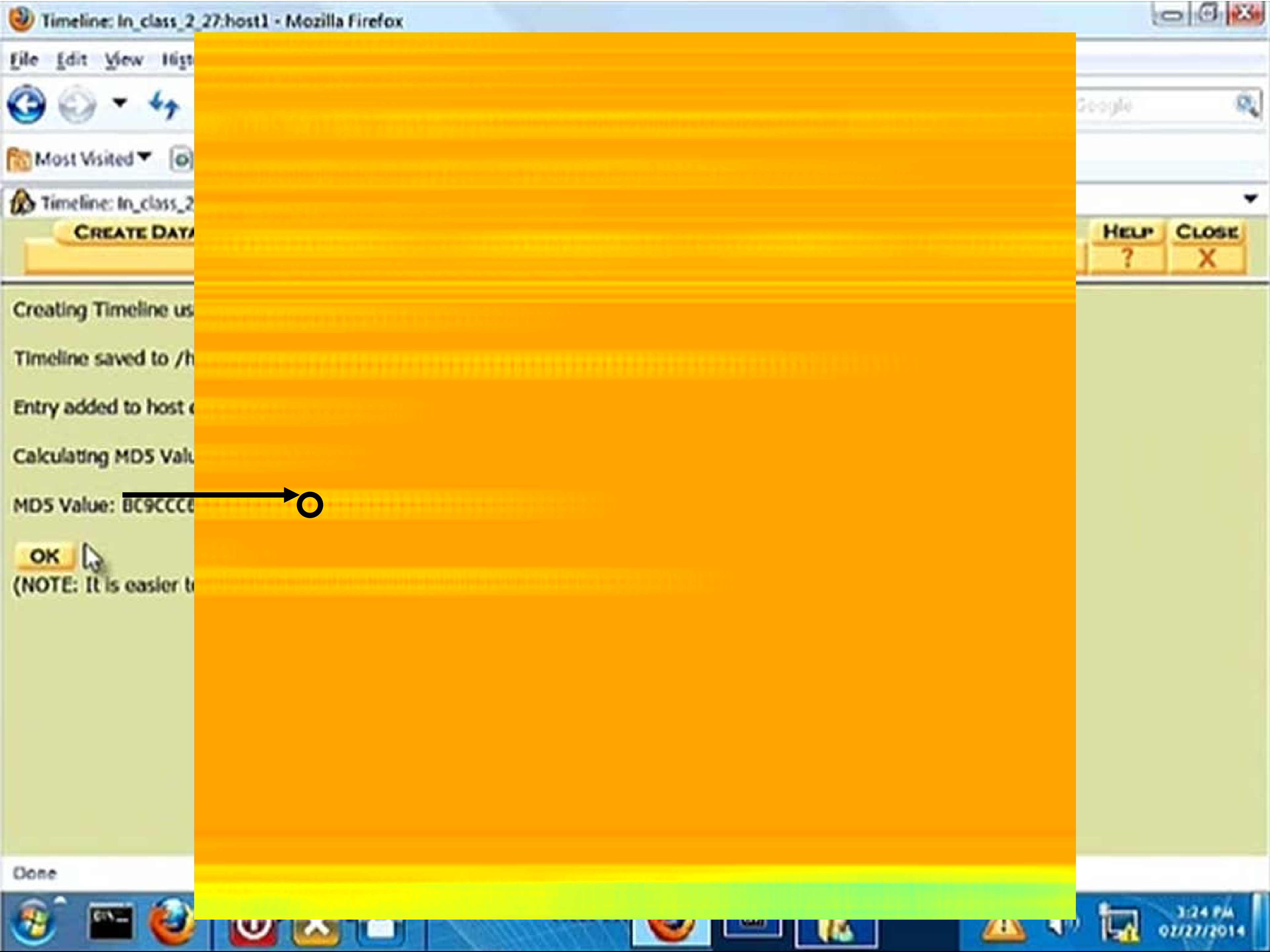
Timeline saved to /home/examiner/Autopsy/In_class_2_27/host1/output/all.txt

Entry added to host config file

Calculating MD5 Value

MD5 Value: 0C9CCC0A1240EF4585230B8901820B64

(NOTE: It is easier to view the timeline in a text editor than here)



Creating Timeline us

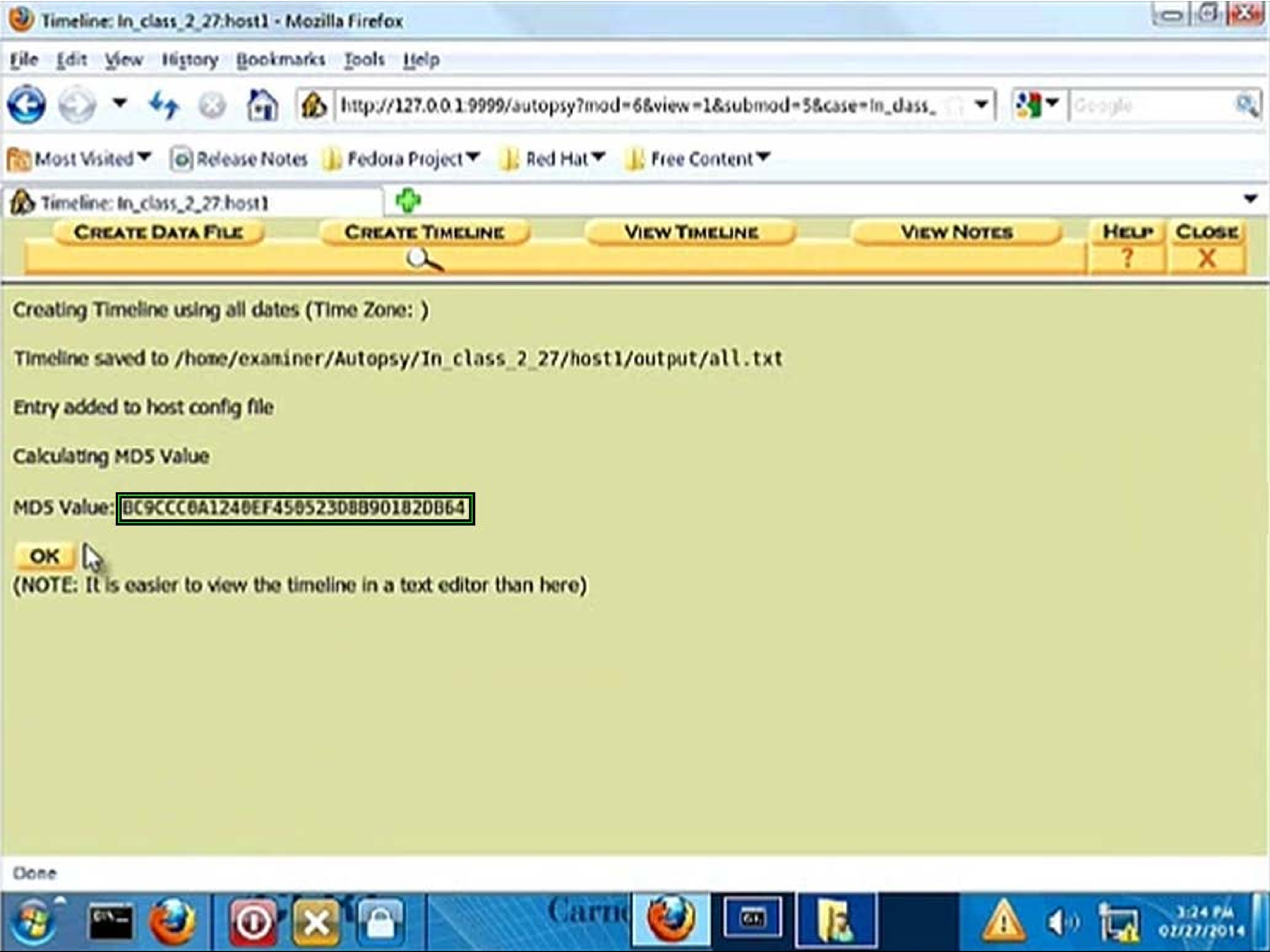
Timeline saved to /h

Entry added to host c

Calculating MD5 Valu

MD5 Value: BC9CCCE

(NOTE: It is easier t


Timeline: In_class_2_27:host1 - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://127.0.0.1:9999/autopsy?mod=6&view=1&submod=5&case=In_class_
Google
Most Visited Release Notes Fedora Project Red Hat Free Content
Timeline: In_class_2_27:host1
CREATE DATA FILE
CREATE TIMELINE
VIEW TIMELINE
VIEW NOTES
HELP
?
CLOSE
X

Creating Timeline using all dates (Time Zone:)

Timeline saved to /home/examiner/Autopsy/In_class_2_27/host1/output/all.txt

Entry added to host config file

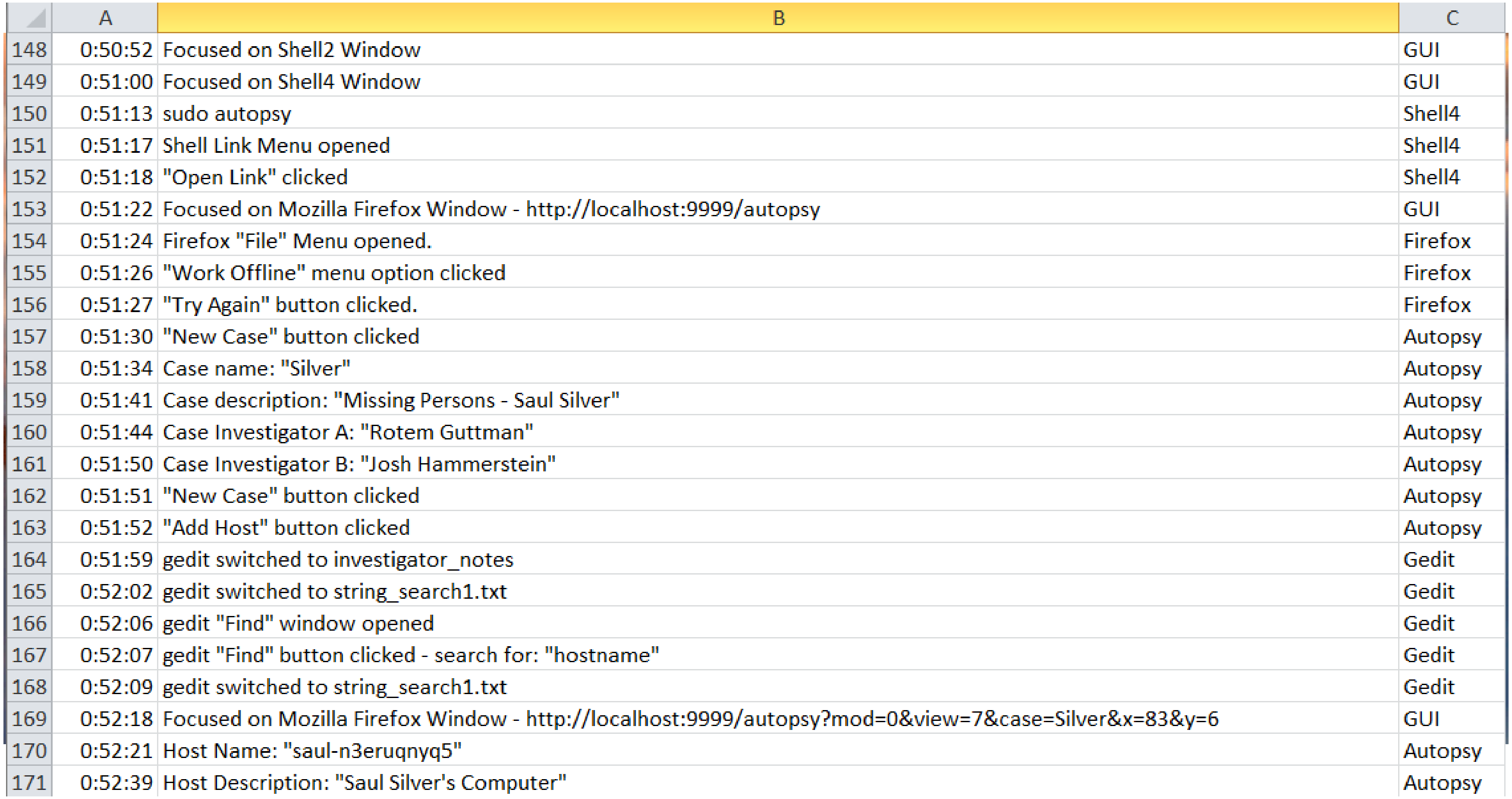
Calculating MD5 Value

MD5 Value: BC9CCC0A1240EF450523088901820B64

OK

(NOTE: It is easier to view the timeline in a text editor than here)

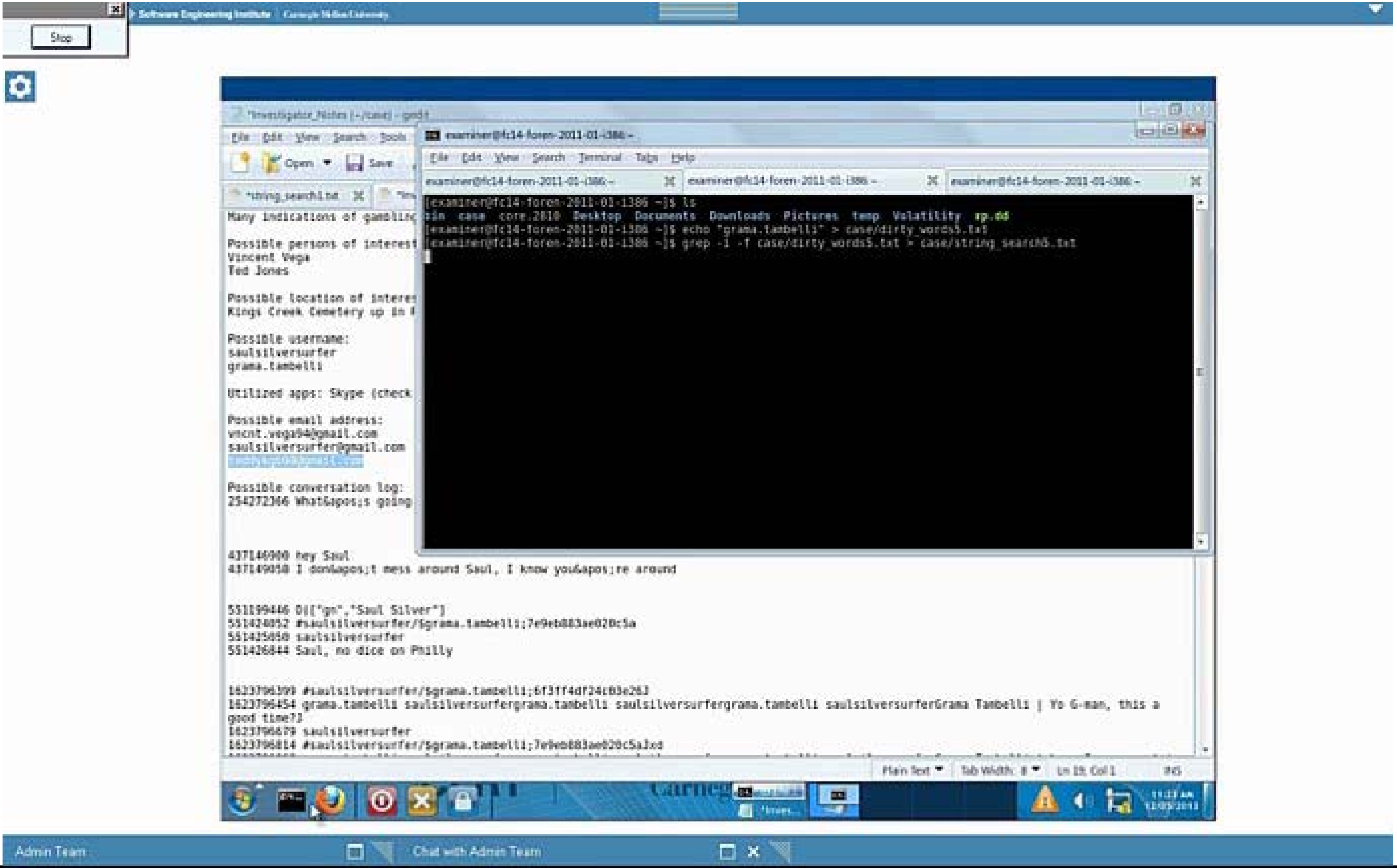
ACE Vision Output



	A	B	C
148	0:50:52	Focused on Shell2 Window	GUI
149	0:51:00	Focused on Shell4 Window	GUI
150	0:51:13	sudo autopsy	Shell4
151	0:51:17	Shell Link Menu opened	Shell4
152	0:51:18	"Open Link" clicked	Shell4
153	0:51:22	Focused on Mozilla Firefox Window - http://localhost:9999/autopsy	GUI
154	0:51:24	Firefox "File" Menu opened.	Firefox
155	0:51:26	"Work Offline" menu option clicked	Firefox
156	0:51:27	"Try Again" button clicked.	Firefox
157	0:51:30	"New Case" button clicked	Autopsy
158	0:51:34	Case name: "Silver"	Autopsy
159	0:51:41	Case description: "Missing Persons - Saul Silver"	Autopsy
160	0:51:44	Case Investigator A: "Rotem Guttman"	Autopsy
161	0:51:50	Case Investigator B: "Josh Hammerstein"	Autopsy
162	0:51:51	"New Case" button clicked	Autopsy
163	0:51:52	"Add Host" button clicked	Autopsy
164	0:51:59	gedit switched to investigator_notes	Gedit
165	0:52:02	gedit switched to string_search1.txt	Gedit
166	0:52:06	gedit "Find" window opened	Gedit
167	0:52:07	gedit "Find" button clicked - search for: "hostname"	Gedit
168	0:52:09	gedit switched to string_search1.txt	Gedit
169	0:52:18	Focused on Mozilla Firefox Window - http://localhost:9999/autopsy?mod=0&view=7&case=Silver&x=83&y=6	GUI
170	0:52:21	Host Name: "saul-n3eruqnyq5"	Autopsy
171	0:52:39	Host Description: "Saul Silver's Computer"	Autopsy

*Confidence measures associated with each row omitted.

Visualization: Synchronized Data



Stop
Software Engineering Institute | Carnegie Mellon University
*Investigator_Notes (~/case) - gedit
File Edit View Search Tools
Open Save
*string_search1.txt
examiner@fc14-foren-2011-01-i386:~
File Edit View Search Terminal Tabs Help
examiner@fc14-foren-2011-01-i386:~
examiner@fc14-foren-2011-01-i386:~
examiner@fc14-foren-2011-01-i386:~
Plain Text
Tab Width: 8
Ln 19, Col 1
INS
11:23 AM
12/05/2013
Admin Team
Chat with Admin Team

```
[examiner@fc14-foren-2011-01-1386 ~]$ ls
bin  case  core.2810  Desktop  Documents  Downloads  Pictures  temp  Volatility  xp.dd
[examiner@fc14-foren-2011-01-1386 ~]$ echo "grama.tambelli" > case/dirty_words5.txt
[examiner@fc14-foren-2011-01-1386 ~]$ grep -i -f case/dirty_words5.txt > case/string_search5.txt
```

```
Many indications of gambling

Possible persons of interest
Vincent Vega
Ted Jones

Possible location of interes
Kings Creek Cemetery up in 

Possible username:
saulsilversurfer
grama.tambelli

Utilized apps: Skype (check

Possible email address:
vncnt.vega94@gmail.com
saulsilversurfer@gmail.com
[illegible]

Possible conversation log:
254272366 What&apos;s going



437146900 hey Saul
437149058 I don&apos;t mess around Saul, I know you&apos;re around


551199446 D([“gn”,"Saul Silver"]
551424052 #saulsilversurfer/$grama.tambelli;7e9eb883ae020c5a
551425050 saulsilversurfer
551426844 Saul, no dice on Philly


1623796399 #saulsilversurfer/$grama.tambelli;6f3ff4df24c03e26J
1623796454 grama.tambelli saulsilversurfergrama.tambelli saulsilversurfergrama.tambelli saulsilversurferGrama Tambelli | Yo G-man, this a
good time?J
1623796679 saulsilversurfer
1623796814 #saulsilversurfer/$grama.tambelli;7e9eb883ae020c5aJxd
```

Focused on Shell2 Window
(GUI)

ACE-Eval

Primary Collaborator:
Professor Geoffrey Gordon

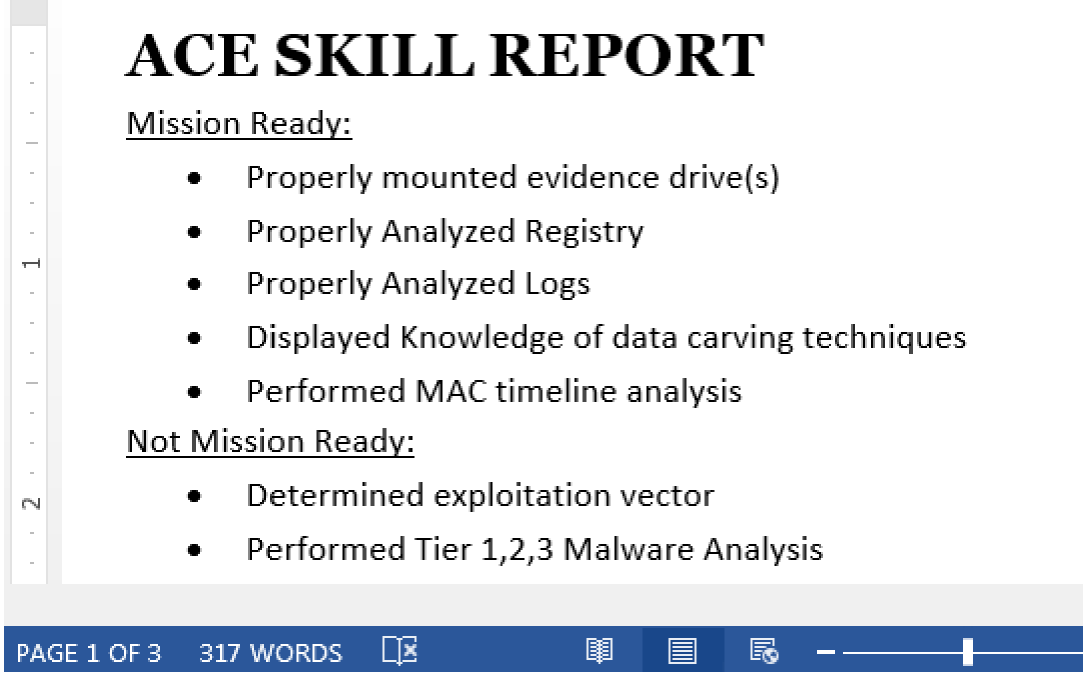
CMU Machine Learning Department

Development

Requires Categorized Data

- Evaluator driven categorization (Training data)
- Hybrid solution required
  - Differing KSA Complexity
    - Simple Binary Detection
    - Path Analysis
    - Hidden Markov Models
    - Frequency Analysis
  - Automated Anomaly Detection
    - Human Intervention

ACE Skill Report



ACE SKILL REPORT

Mission Ready:

- Properly mounted evidence drive(s)
- Properly Analyzed Registry
- Properly Analyzed Logs
- Displayed Knowledge of data carving techniques
- Performed MAC timeline analysis

Not Mission Ready:

- Determined exploitation vector
- Performed Tier 1,2,3 Malware Analysis

Output of Evaluation System

- Determines mission-readiness
- Isolates deficiencies
- Recommends additional training
- Automated remediation plans

Future Work

- **High Transition Potential**
  - Compatible with existing work
  - CPT integration
  - Additional job roles
- **FY16 Plans**
  - Evaluation of analyst to DoD partner’s satisfaction
  - Identification of additional roles
  - Integration of ACE capabilities with AC3 processes
- **Post FY16**
  - Integration with PWP work
  - Role expansion
  - Squad level evaluation