# Security Paintings

***How do you convey information when you don't really know what's happening?***

Jonathan Grier
ACSAC 2012

# Legal Disclaimer

Some technologies discussed in this presentation may be patent pending.

| Status | Website | Rating | # Webpages | Webpages in % | See Webpages! |
|---|---|---|---|---|---|
| | movies.netflix.com | Adult | 11 | 27% | Details |

## movies.netflix.com

**Rating:** Adult

| Webpages | Rating | Time |
|---|---|---|
| http://movies.netflix.com/WiHome | Everybody | 13:09 07/10/2011 |
| http://movies.netflix.com/WiSearch?oq=blade+r&ac_p... | Everybody | 13:08 07/10/2011 |
| http://movies.netflix.com/JSON/AutoCompleteSearch?... | Everybody | 13:08 07/10/2011 |
| http://movies.netflix.com/JSON/AutoCompleteSearch?... | Everybody | 13:08 07/10/2011 |
| http://movies.netflix.com/JSON/AutoCompleteSearch?... | Everybody | 13:08 07/10/2011 |
| http://movies.netflix.com/JSON/AutoCompleteSearch?... | Everybody | 13:08 07/10/2011 |
| http://movies.netflix.com/JSON/AutoCompleteSearch?... | Pre-Teen | 13:08 07/10/2011 |
| http://movies.netflix.com/JSON/AutoCompleteSearch?... | Everybody | 13:08 07/10/2011 |
| http://movies.netflix.com/JSON/AutoCompleteSearch?... | Everybody | 13:08 07/10/2011 |
| http://movies.netflix.com/WiContentPage?pn=2&csid=... | Adult | 13:07 07/10/2011 |

# Adult

Time spent: less than 10 minutes
Webpages visited: 1

1. **Pornography - Wikipedia, the free encyclopedia** http://en.wikipedi
   Details *en.wikipedia.org*

# Drugs, Alcohol & Tobacco

Time spent: less than 10 minutes
Webpages visited: 5

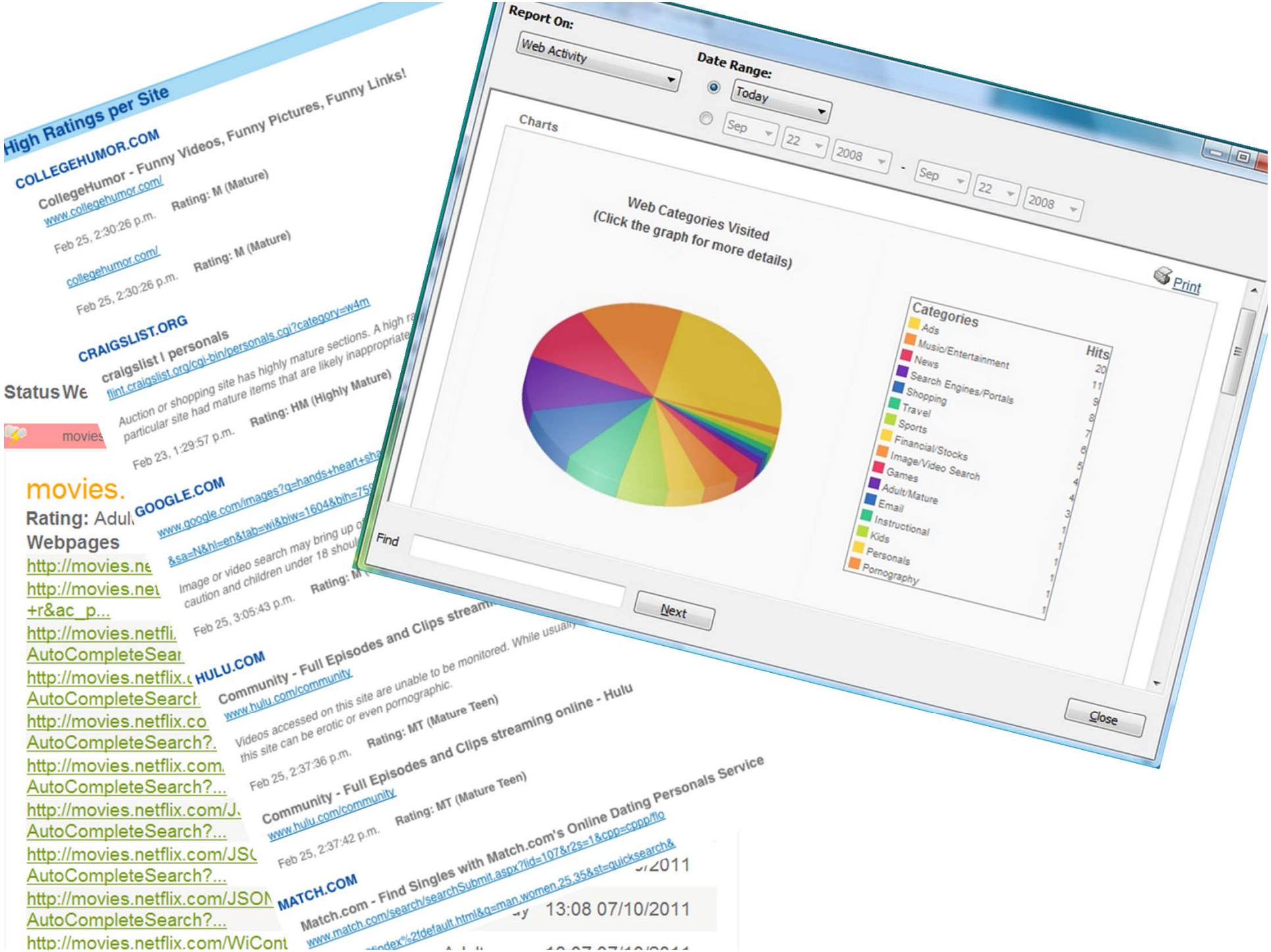
1. **Pornography - Wikipedia, the free encyclopedia** http://en.wikipedi
   Details *en.wikipedia.org*

2. **How do people get marijuana if its illegal? - Yahoo! Answers** http://answers.ya
   Details *I know marijuana is illegal. But I want to know ho…*

3. **Drugs.com | Prescription Drug Information, Interactions & Side Effects** http://www.drugs.
   Details *Prescription drug information and news for professionals and consumers. Search our drug database for comprehensive prescription and patient information on 24,000 drugs online*

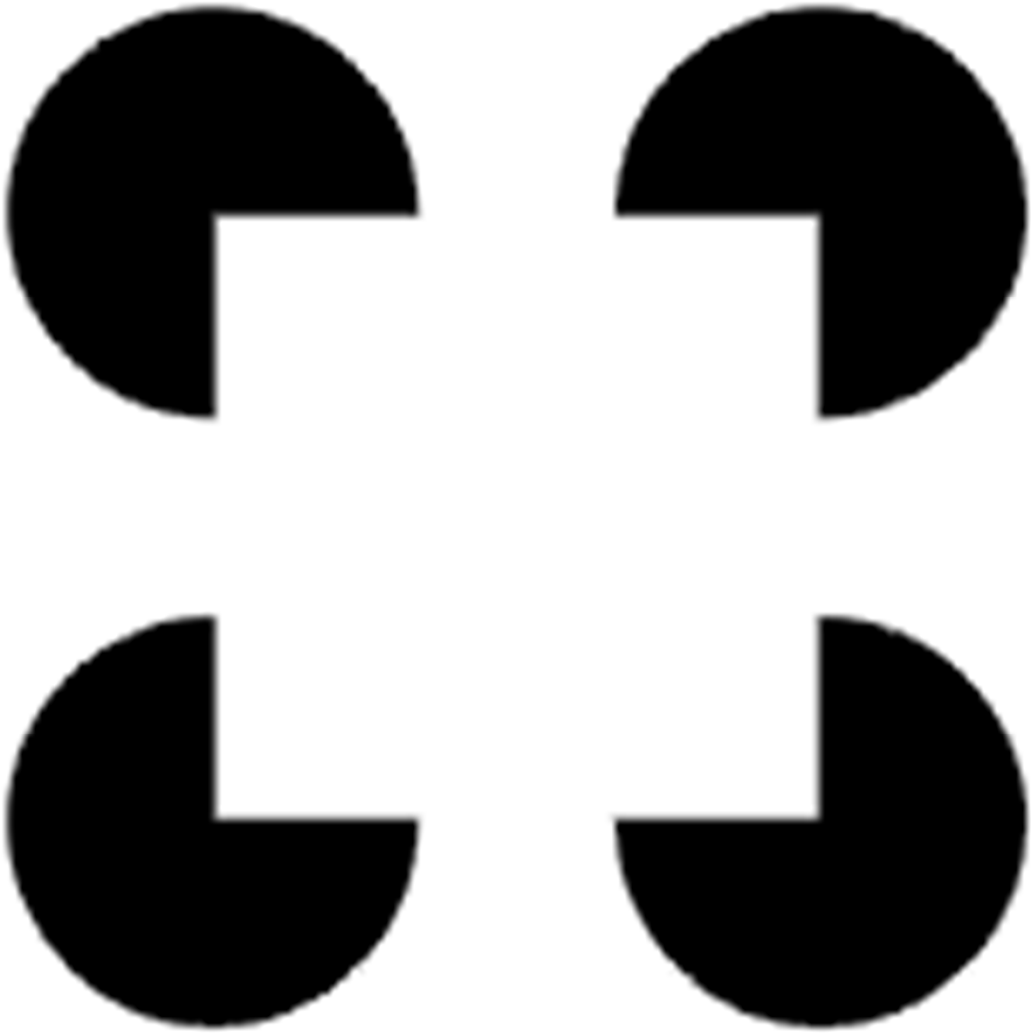
**WeBeHigh.com Los Angeles, CA** http://www.webeh
**Marijuana prices and where to buy weed**


***"Online safety parents and kids can agree on"***


High Ratings per Site
COLLEGEHUMOR.COM
CollegeHumor - Funny Videos, Funny Pictures, Funny Links!
www.collegehumor.com/
Feb 25, 2:30:26 p.m. Rating: M (Mature)
collegehumor.com/
Feb 25, 2:30:26 p.m. Rating: M (Mature)
CRAIGSLIST.ORG
craigslist | personals
flint.craigslist.org/cgi-bin/personals.cgi?category=w4m
Auction or shopping site has highly mature sections. A high r
particular site had mature items that are likely inappropriate
Feb 23, 1:29:57 p.m. Rating: HM (Highly Mature)
Status We
movies
movies.
Rating: Adul
Webpages
http://movies.ne
http://movies.net
+r&ac_p...
http://movies.netfli
AutoCompleteSear
http://movies.netflix.
AutoCompleteSearch
http://movies.netflix.co
AutoCompleteSearch?.
http://movies.netflix.com
AutoCompleteSearch?...
http://movies.netflix.com/J
AutoCompleteSearch?...
http://movies.netflix.com/JS
AutoCompleteSearch?...
http://movies.netflix.com/JSON
AutoCompleteSearch?...
http://movies.netflix.com/WiCont
GOOGLE.COM
www.google.com/images?q=hands+heart+sha
&sa=N&hl=en&tab=wi&biw=1604&bih=75
Image or video search may bring up
caution and children under 18 shou
Feb 25, 3:05:43 p.m. Rating: M
HULU.COM
Community - Full Episodes and Clips stream
www.hulu.com/community
Videos accessed on this site are unable to be monitored. While usually
this site can be erotic or even pornographic.
Feb 25, 2:37:36 p.m. Rating: MT (Mature Teen)
Community - Full Episodes and Clips streaming online - Hulu
www.hulu.com/community
Feb 25, 2:37:42 p.m. Rating: MT (Mature Teen)
MATCH.COM
Match.com - Find Singles with Match.com's Online Dating Personals Service
www.match.com/search/searchSubmit.aspx?lid=107&r2s=1&cpp=cppp/flo
index%2Fdefault.html&g=man,women,25,35&st=quicksearch&
13:08 07/10/2011
Report On:
Web Activity
Date Range:
Today
Sep 22 2008 - Sep 22 2008
Charts
Web Categories Visited
(Click the graph for more details)
Print
Categories
Hits
Ads 20
Music/Entertainment 11
News 9
Search Engines/Portals 8
Shopping 7
Travel 6
Sports 5
Financial/Stocks 4
Image/Video Search 4
Games 3
Adult/Mature 1
Email 1
Instructional 1
Kids 1
Personals 1
Pornography 1
Find
Next
Close

# What data do I have?
# How can I present it?


**What *conclusions* interest me?**
**How can I *perceive* them?**



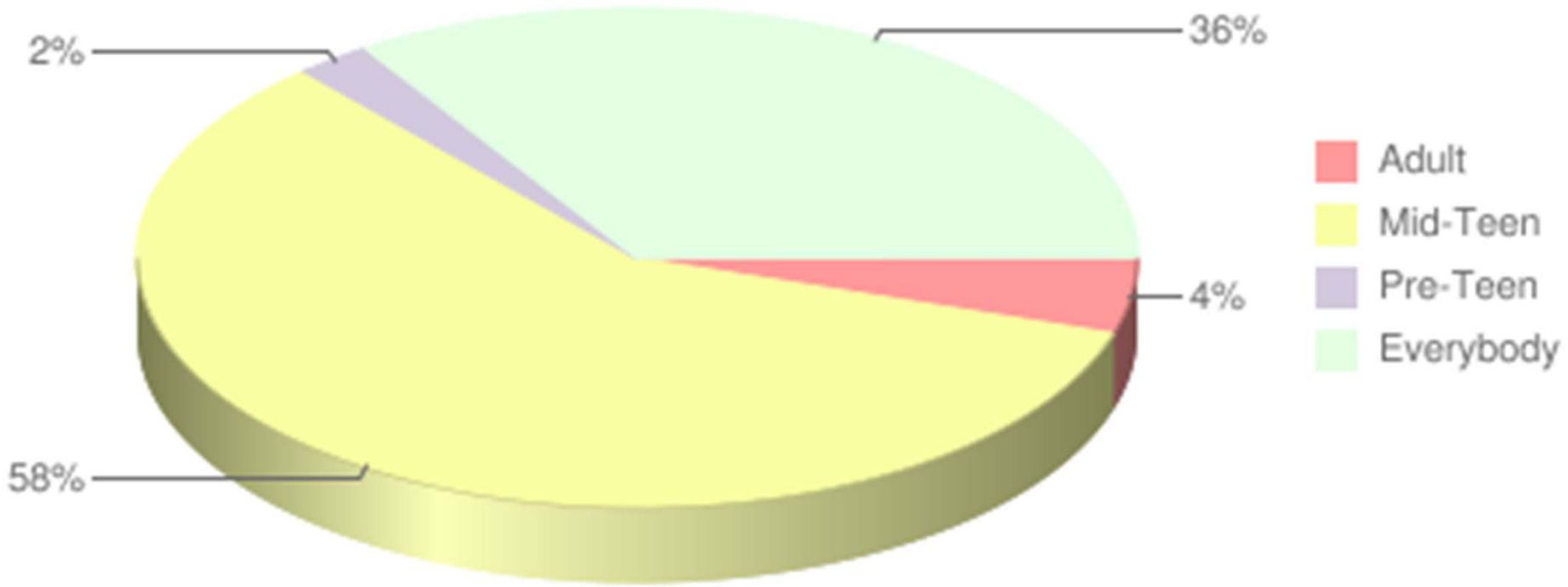
| Status | Website | Rating | # Webpages | Webpages in % | See Webpages! |
|---|---|---|---|---|---|
| | movies.netflix.com | Adult | 11 | 27% | Details |

## movies.netflix.com

**Rating:** Adult

| Webpages | Rating | Time |
|---|---|---|
| http://movies.netflix.com/WiHome | Everybody | 13:09 07/10/2011 |
| http://movies.netflix.com/WiSearch?oq=blade+r&ac_p... | Everybody | 13:08 07/10/2011 |
| http://movies.netflix.com/JSON/AutoCompleteSearch?... | Everybody | 13:08 07/10/2011 |
| http://movies.netflix.com/JSON/AutoCompleteSearch?... | Everybody | 13:08 07/10/2011 |
| http://movies.netflix.com/JSON/AutoCompleteSearch?... | Everybody | 13:08 07/10/2011 |
| http://movies.netflix.com/JSON/AutoCompleteSearch?... | Everybody | 13:08 07/10/2011 |
| http://movies.netflix.com/JSON/AutoCompleteSearch?... | Pre-Teen | 13:08 07/10/2011 |
| http://movies.netflix.com/JSON/AutoCompleteSearch?... | Everybody | 13:08 07/10/2011 |
| http://movies.netflix.com/JSON/AutoCompleteSearch?... | Everybody | 13:08 07/10/2011 |
| http://movies.netflix.com/WiContentPage?pn=2&csid=... | Adult | 13:07 07/10/2011 |

# Rating summary - displays surfing activities sorte

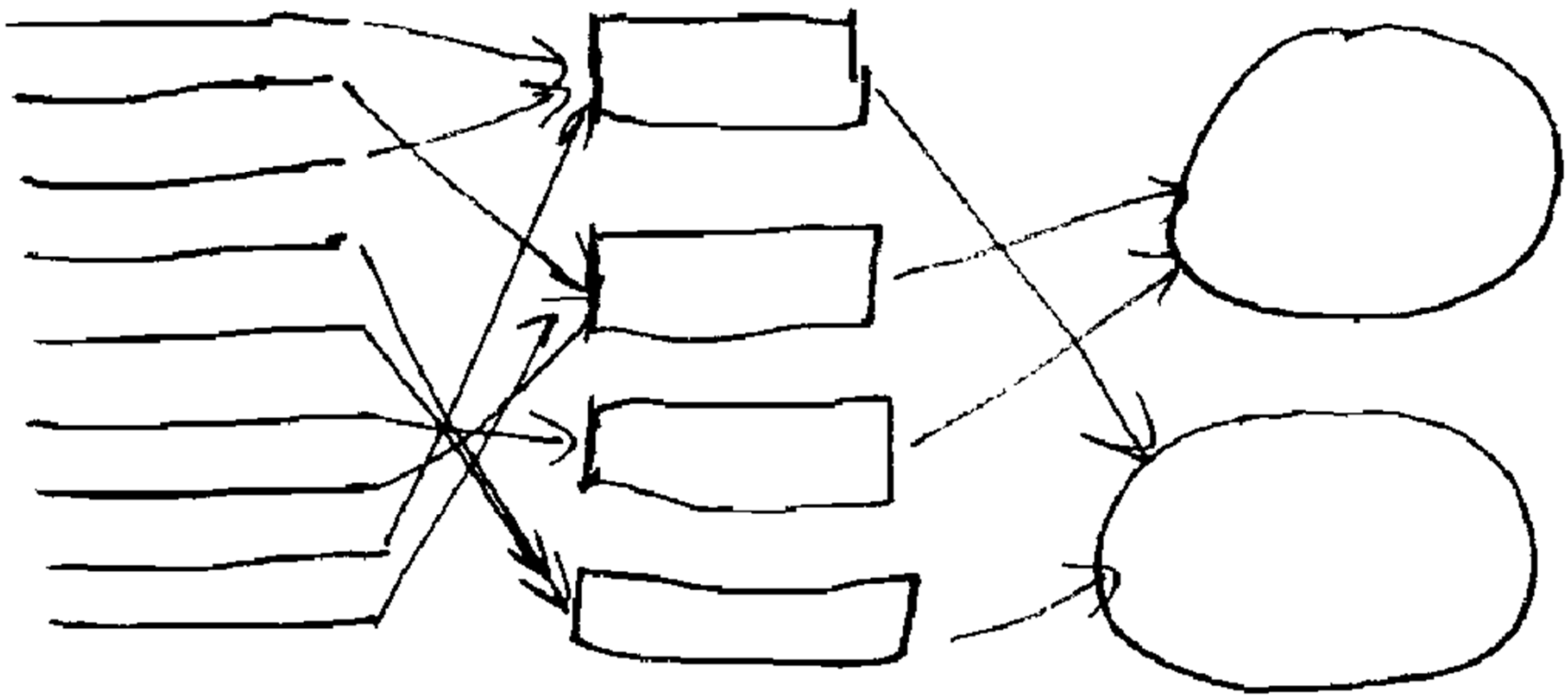


1. **Only High level data is *interesting*.**
   **But only Low level data is *credible*.**

2. **Uncertain Ordering**

3. **Want Repeated Patterns**

4. **Want Context**



# Adult

Time spent: less than 10 minutes
Webpages visited: 1

| | | |
|---|---|---|
| 1. | **Pornography - Wikipedia, the free encyclopedia**<br>Details *en.wikipedia.org* | http://en.wikipedia.org/wiki/P... |

# Drugs, Alcohol & Tobacco

Time spent: less than 10 minutes
Webpages visited: 5

| | | |
|---|---|---|
| 1. | **Pornography - Wikipedia, the free encyclopedia**<br>Details *en.wikipedia.org* | http://en.wikipedia.org/wiki/P... |
| 2. | **How do people get marijuana if its illegal? - Yahoo! Answers**<br>Details *I know marijuana is illegal. But I want to know ho...* | http://answers.yahoo.com/quest... |
| 3. | **Drugs.com \| Prescription Drug Information, Interactions & Side Effects**<br>Details *Prescription drug information and news for professionals and consumers. Search our drug database for comprehensive prescription and patient information on 24,000 drugs online* | http://www.drugs.com/ |
| | **WeBeHigh.com Los Angeles, CA**<br>**Marijuana prices and where to buy weed** | http://www.webehigh.com/city/d... |

# Alcohol

3 hours (23 sites) this week

First Visit: 3 months ago
Time Spent: 2 hours per week

1. **Budweiser - King of Beers** www.budweiser.com
Details
*Budwesier: the Great American Lager... Budweiser **beer**... America's best **beer**.*

2. **Coors Light** www.coorslight.com
Details
*Coors Light: You must be 21 or over to visit this site. Please verify...*

3. **Dr Vino's wine blog** www.drvino.com
NEW SITE
Details
*A spirited **wine** blog with independent picks... **wine** maps...*

4. **Consumer Reports - Wine Information** www.consumerreports.org/cro/food/...
Details
*Get information on **wines** from the unbiased, independent experts.*

5. **Miller Lite - Wikipedia, the free...** en.wikipedia.org/wiki/Miller_Lite
Details
*Miller Lite is a 4.2%... Sibling **beers** include Miller Genuide Draft and Miller Regular...*

6 - 23. Show 18 more Alcohol sites...

# Sports

8 hours (105 sites) this week
INCREASED ACTIVITY

First Visit: 6 months ago
Time Spent: 4 hours per week

1. **NBA** www.nba.org
Details
*National **Basketball** Association. Your source...*

2. **Sports Illustrated** sportsillustrated.com
Details
***Sports** Illustrated: The best source for info on all your favorite **sports**.*

3. **Yankees** facebook.com/pages?yankees
Details
*Welcome to the New York Yankees Facebook page*

4 - 105. Show 102 more Sports sites...

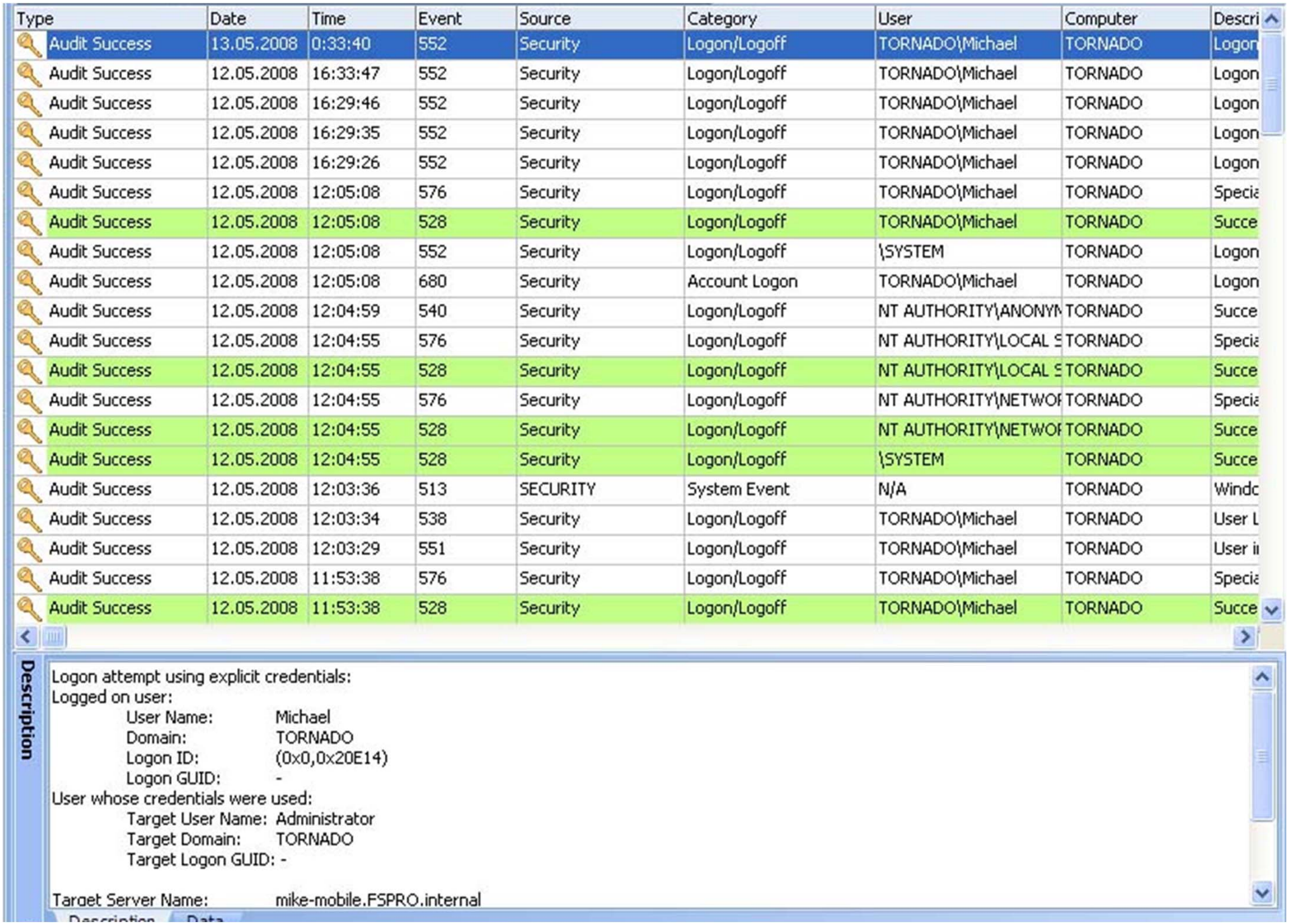

LIBERTY
IN GOD WE TRUST
1945


LIBERTY
IN GOD WE TRUST
1945

LIBERTY
IN GOD WE TRUST
1945

LIBERTY
IN GOD WE TRUST
1945

# Activity

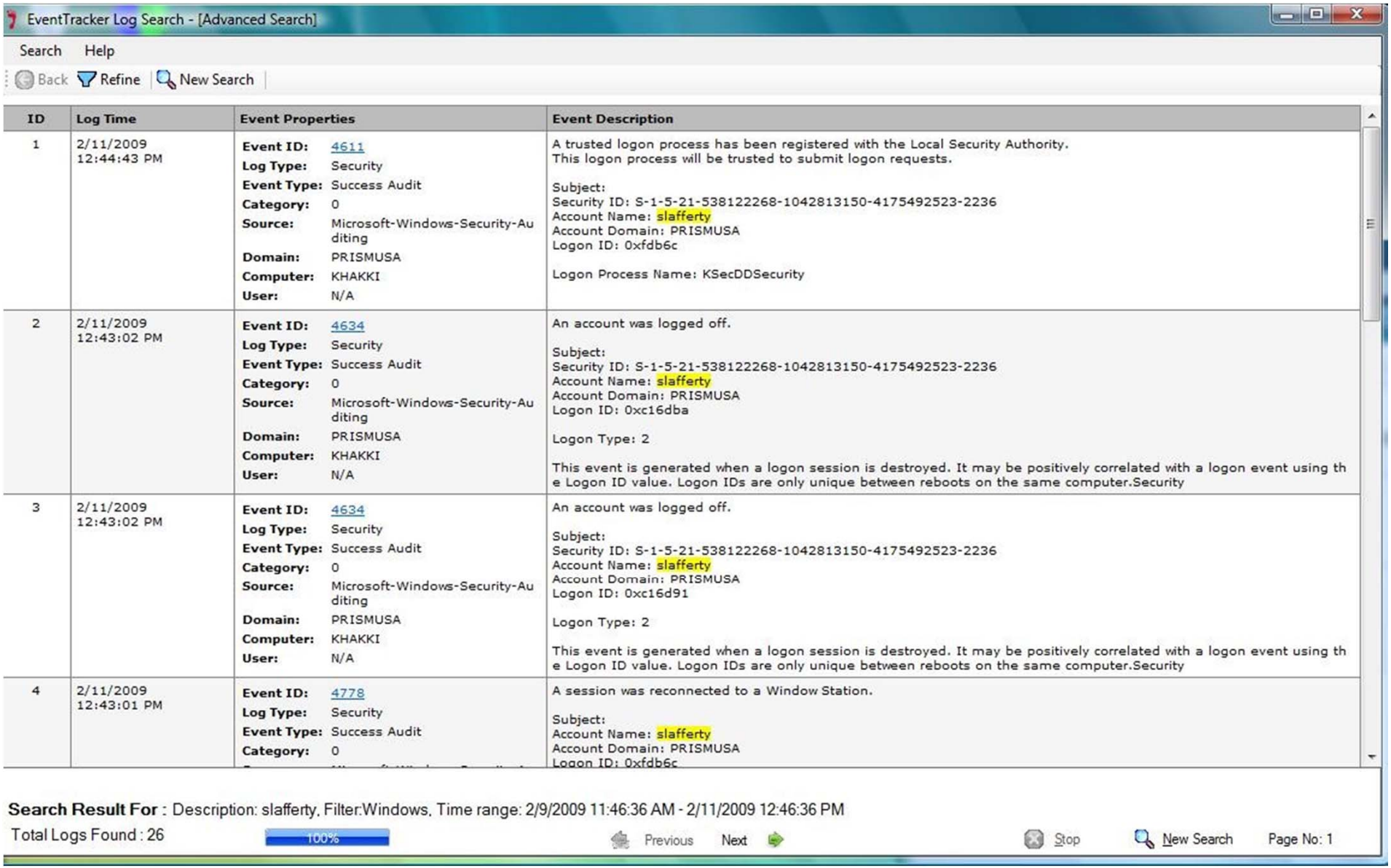


| Type | Date | Time | Event | Source | Category | User | Computer | Descri |
|---|---|---|---|---|---|---|---|---|
| Audit Success | 13.05.2008 | 0:33:40 | 552 | Security | Logon/Logoff | TORNADO\Michael | TORNADO | Logon |
| Audit Success | 12.05.2008 | 16:33:47 | 552 | Security | Logon/Logoff | TORNADO\Michael | TORNADO | Logon |
| Audit Success | 12.05.2008 | 16:29:46 | 552 | Security | Logon/Logoff | TORNADO\Michael | TORNADO | Logon |
| Audit Success | 12.05.2008 | 16:29:35 | 552 | Security | Logon/Logoff | TORNADO\Michael | TORNADO | Logon |
| Audit Success | 12.05.2008 | 16:29:26 | 552 | Security | Logon/Logoff | TORNADO\Michael | TORNADO | Logon |
| Audit Success | 12.05.2008 | 12:05:08 | 576 | Security | Logon/Logoff | TORNADO\Michael | TORNADO | Specia |
| Audit Success | 12.05.2008 | 12:05:08 | 528 | Security | Logon/Logoff | TORNADO\Michael | TORNADO | Succe |
| Audit Success | 12.05.2008 | 12:05:08 | 552 | Security | Logon/Logoff | \SYSTEM | TORNADO | Logon |
| Audit Success | 12.05.2008 | 12:05:08 | 680 | Security | Account Logon | TORNADO\Michael | TORNADO | Logon |
| Audit Success | 12.05.2008 | 12:04:59 | 540 | Security | Logon/Logoff | NT AUTHORITY\ANONYM | TORNADO | Succe |
| Audit Success | 12.05.2008 | 12:04:55 | 576 | Security | Logon/Logoff | NT AUTHORITY\LOCAL S | TORNADO | Specia |
| Audit Success | 12.05.2008 | 12:04:55 | 528 | Security | Logon/Logoff | NT AUTHORITY\LOCAL S | TORNADO | Succe |
| Audit Success | 12.05.2008 | 12:04:55 | 576 | Security | Logon/Logoff | NT AUTHORITY\NETWOF | TORNADO | Specia |
| Audit Success | 12.05.2008 | 12:04:55 | 528 | Security | Logon/Logoff | NT AUTHORITY\NETWOF | TORNADO | Succe |
| Audit Success | 12.05.2008 | 12:04:55 | 528 | Security | Logon/Logoff | \SYSTEM | TORNADO | Succe |
| Audit Success | 12.05.2008 | 12:03:36 | 513 | SECURITY | System Event | N/A | TORNADO | Windc |
| Audit Success | 12.05.2008 | 12:03:34 | 538 | Security | Logon/Logoff | TORNADO\Michael | TORNADO | User L |
| Audit Success | 12.05.2008 | 12:03:29 | 551 | Security | Logon/Logoff | TORNADO\Michael | TORNADO | User ir |
| Audit Success | 12.05.2008 | 11:53:38 | 576 | Security | Logon/Logoff | TORNADO\Michael | TORNADO | Specia |
| Audit Success | 12.05.2008 | 11:53:38 | 528 | Security | Logon/Logoff | TORNADO\Michael | TORNADO | Succe |

Description

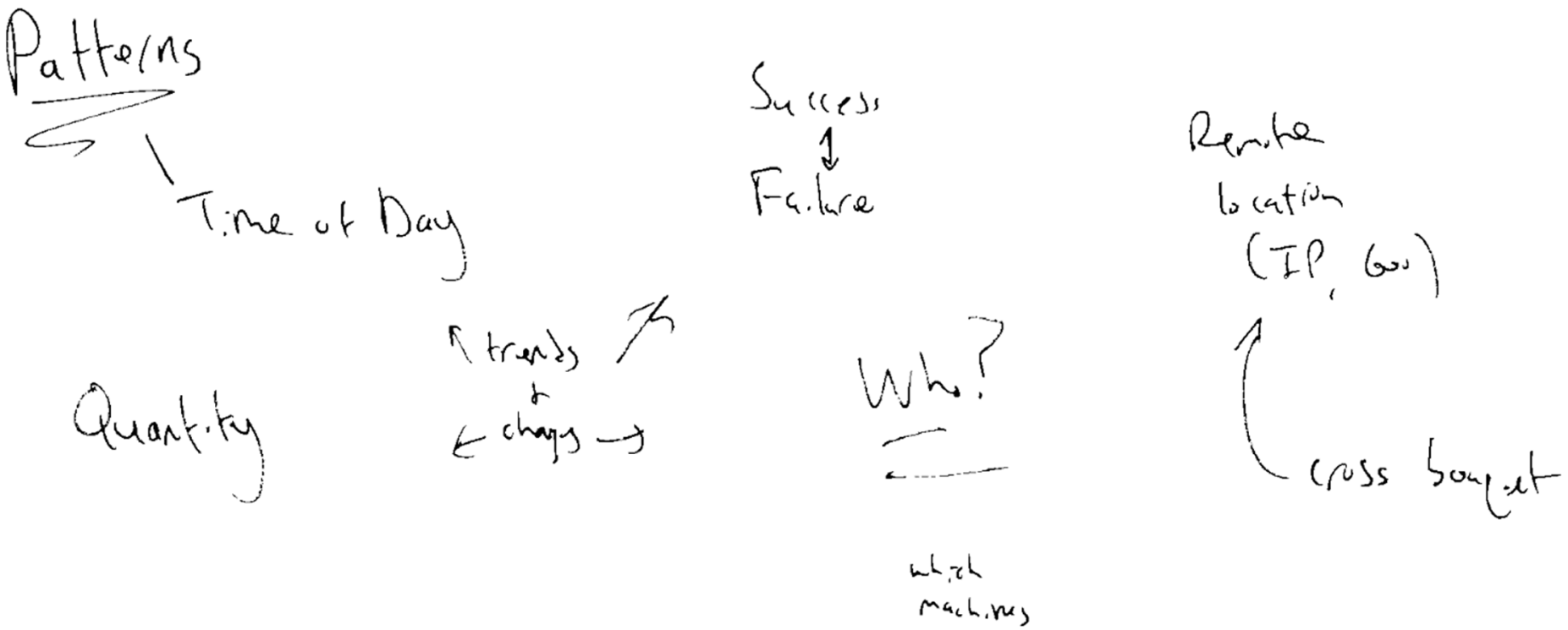
Logon attempt using explicit credentials:
Logged on user:
User Name: Michael
Domain: TORNADO
Logon ID: (0x0,0x20E14)
Logon GUID: -
User whose credentials were used:
Target User Name: Administrator
Target Domain: TORNADO
Target Logon GUID: -

Target Server Name: mike-mobile.FSPRO.internal


EventTracker Log Search - [Advanced Search]
Search
Help
Back
Refine
New Search
ID
Log Time
Event Properties
Event Description
1
2/11/2009 12:44:43 PM
Event ID: 4611
Log Type: Security
Event Type: Success Audit
Category: 0
Source: Microsoft-Windows-Security-Auditing
Domain: PRISMUSA
Computer: KHAKKI
User: N/A
A trusted logon process has been registered with the Local Security Authority.
This logon process will be trusted to submit logon requests.
Subject:
Security ID: S-1-5-21-538122268-1042813150-4175492523-2236
Account Name: slafferty
Account Domain: PRISMUSA
Logon ID: 0xfdb6c
Logon Process Name: KSecDDSecurity
2
2/11/2009 12:43:02 PM
Event ID: 4634
Log Type: Security
Event Type: Success Audit
Category: 0
Source: Microsoft-Windows-Security-Auditing
Domain: PRISMUSA
Computer: KHAKKI
User: N/A
An account was logged off.
Subject:
Security ID: S-1-5-21-538122268-1042813150-4175492523-2236
Account Name: slafferty
Account Domain: PRISMUSA
Logon ID: 0xc16dba
Logon Type: 2
This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.Security
3
2/11/2009 12:43:02 PM
Event ID: 4634
Log Type: Security
Event Type: Success Audit
Category: 0
Source: Microsoft-Windows-Security-Auditing
Domain: PRISMUSA
Computer: KHAKKI
User: N/A
An account was logged off.
Subject:
Security ID: S-1-5-21-538122268-1042813150-4175492523-2236
Account Name: slafferty
Account Domain: PRISMUSA
Logon ID: 0xc16d91
Logon Type: 2
This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.Security
4
2/11/2009 12:43:01 PM
Event ID: 4778
Log Type: Security
Event Type: Success Audit
Category: 0
A session was reconnected to a Window Station.
Subject:
Account Name: slafferty
Account Domain: PRISMUSA
Logon ID: 0xfdb6c
Search Result For : Description: slafferty, Filter:Windows, Time range: 2/9/2009 11:46:36 AM - 2/11/2009 12:46:36 PM
Total Logs Found : 26
100%
Previous
Next
Stop
New Search
Page No: 1

**What *conclusions***
**do *they* want to form?**

**How can they**
***see* them?**


Patterns
Time of Day
Quantity
trends
changes
Success
Failure
Who?
which machines
Remote location (IP, Geo)
cross basket

## Conclusions

Multiple *levels* of data

## Patterns

Make *bouquets* of *examples*

## Context

Mix in *lateral info*

Escape the ~~*schema*~~

Robert

Harrison

successfull

75 logins

this week

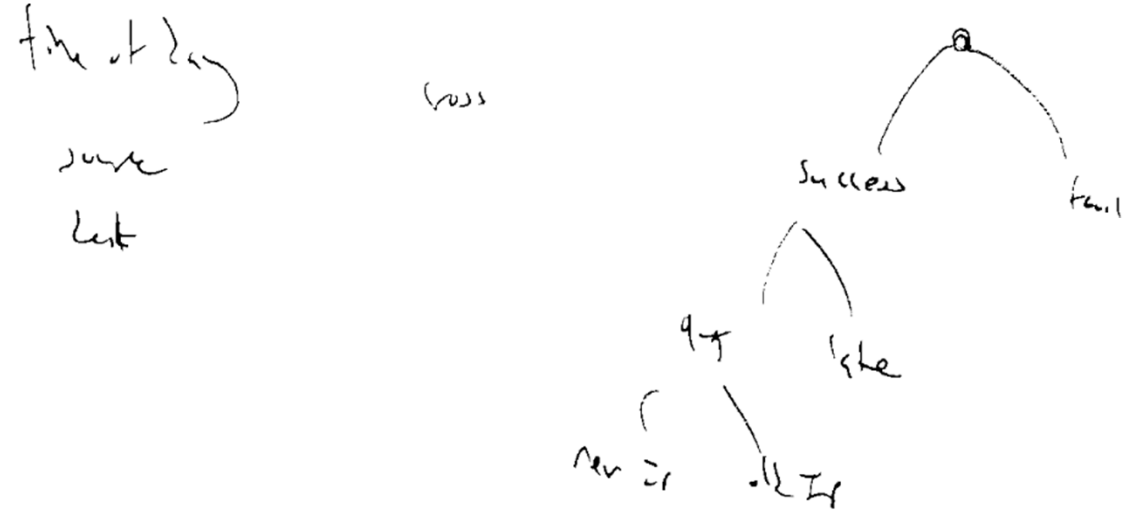
(typically 8 per week)

failed

13 failed attempts

this week

(typically 6 per week)



# Robert Harrison

SENIOR VP, MARKETING
rharrison@secureco.com

**75** logins this week
(typically about 90/wk)

**23** failed attempts this week
(typically about 10/wk)

**UNUSUAL ACTIVITY this week:**

17 logins from new IP 34.53.104.32
(Verizon FiOS from Los Angeles, CA)

- Wed Dec 13 3:43pm to ROLF9
- Thu Dec 14 9:15am to ROLF9
- Thu Dec 14 11:40pm to ROLF9
- Fri Dec 15 9:45am to ROLF9
- Show 13 more logins...

**NORMAL ACTIVITY this week:** When did this happen before?

- 19 failed attempts from IP 101.23.86.32 (Odessa, Ukraine)
- 4 failed attempts from office
- 51 logins from office
- 7 logins from IP 17.110.8.20 (Comcast from Baltimore, MD)

Looking to hire:
Web Shadow needs
Windows API
programmers

**Questions?**
**Feedback?**

**Please speak to me here at ACSAC,**
**or, if we miss each other:**

**Jonathan Grier**
**jdgrier at vesaria . com**
**443.501.4044 x1**