SAMPLE Investigation RESPONSE

Case Number: 2014-0001
Date opened: Jan 31 2014

ADMINISTRIVIA

Issue:
Report of compromised credentials by Ulric Issac DAWSON

COMPLAINT

Narrative:
2014-Jan-31

WHAT I DID

INVESTIGATOR received a complaint from DAWSON that his user credentials have been compromised. INVESTIGATOR requested clarification from DAWSON on why he believed his account was compromised.

SCOPING the Investigation

NOTE: DAWSON evasive in response

INVESTIGATOR observations separated from facts learned during investigation

INVESTIGATOR restates request and advises that without cooperation from DAWSON this office cannot complete an investigation.

DAWSON disclosed that emails that originated from his DOMAIN account have been harvested and returned to his DOMAIN account. This has occurred in the past and reoccurred this morning. INVESTIGATOR requested that DAWSON supply the examples of the suspected harvested emails.

FACTS

NOTE: DAWSON evasive and reluctant to provide examples required

FACTS

DAWSON supplied two subject line examples:
'When I win this will you come'
'Sadness vs Happiness'

DATA SOURCE UTILIZED

INVESTIGATOR reviewed the PIXIE email Gateway for all traffic to or from DAWSON's Account UID@DOMAIN.COM for 2013-02-01 0000hrs to present.

INVESTIGATOR identified emails with the suspect lines:

2014-01-24 7:02	UID@domain.com	unknsub@shaw.com	FW: When I win this, will you come ?
2014-01-24 7:14	UID@domain.com	unknsub@shaw.com	FW: Sadness vs Happiness
2014-01-24 7:44	unknsub@shaw.com	UID@domain.com	RE: Sadness vs Happiness
2014-01-24 7:44	unknsub@shaw.com	UID@domain.com	RE: When I win this, will you come ?

LOG INFORMATION (irrefutable facts) Corroborating Evidence

NOTE there also the Sadness vs Happiness subject line that goes to a LADYBIRD1@YAHOO.NET account.	INVESTIGATOR Observation
Due to the above evidence supporting DAWSON assertion that his account has been compromised INNVESTIGATOR recommended that DAWSON change his password immediately.	FACTS
INVESTIGATOR queried the OUTLOOK WEB ACCESS (OWA) logs for the date 2013-FEB-01 for UID@DOMAIN.COM	Documentary Evidence (one leads to another PIXIE -> OWA review)
In reviewing the OWA logs access was made to the account of DAWSON from IP address 76.193.130.252 and commands associated with the access, sending and deleting of activities (see attached LOG data).	FACTS
INVESTIGATOR acquired a copy of DAWSON's MAILBOX from the EXCHANGE environment for review.	Documentary Evidence (one leads to another OWA-> Mailbox review)
INVESTIGATOR reviewed the email associated with the Sadness vs Happiness item received into the network from unknsub@shaw.com at 0744 2013-Feb-1. Header information shows email originated from IP address 76.193.130.252. . Same IP was discovered on the second email. (See attached Header documentation)	FACTS
This address corresponds to the OWA access.	FACTS
INVESTIGATOR utilizing an internet IP ADDRESS LOCATOR determined that the 76.193.130.252 is associated with a local residence.	Documentary Evidence FACTS
INVESTIGATOR asked DAWSON his relationship to the unknsub@shaw.com person. DAWSON advised that this person is their cohabiting significant other (CSO).	FACTS
INVESTIGATOR reviewed a further sample from the mailbox of DAWSON and determined that DAWSON was utilizing the corporate email account to maintain a number of personal liaisons that may bring the corporation into disrepute.	FACTS

SAMPLE Investigation RESPONSE

<u>Conclusion</u>:	
Compromise of the account belonging to DAWSON is confirmed.	FINDING / FACT
The evidence suggests that the access to the accounts of DAWSON were done by his CSO. The data from the OWA logs do not support a finding of a security breach to corporate data.	FACT / INVESTIGATOR EXPERIENCE
The emails accessed and returned were associated with personal non work related liaisons.	FACT
Possible explanations for the credential compromise:	
1) Saved Data in a web browser granting access to OWA 2) Poor credential security (written down near asset) 3) Spyware located on home machine which captured logon credentials	INVESTIGATOR EXPERIENCE / most Likely explanations
Chief Information Office advised of inappropriate use of corporate resources by DAWSON.	
File forwarded to Human Resources for follow up review of DAWSON.	TRANSFER OF Authority

SENG460 Instructor Data

Time	Sender	Recipients	Subject
2014-01-24 6:57	UID@domain.com	ladybird1@yahoo.net	Sadness vs Happiness
2014-01-24 6:57	UID@domain.com	ladybird1@yahoo.net	Sadness vs Happiness
2014-01-24 7:00	UID@domain.com	ladybird1@yahoo.net	Happy Tuesday, Baby
2014-01-24 7:02	UID@domain.com	unknsub@shaw.com	FW: When I win this, will you come ?
2014-01-24 7:14	UID@domain.com	unknsub@shaw.com	FW: Sadness vs Happiness
2014-01-24 7:44	unknsub@shaw.com	UID@domain.com	RE: Sadness vs Happiness
2014-01-24 7:44	unknsub@shaw.com	UID@domain.com	RE: When I win this, will you come ?
2014-01-24 8:22	unknsub@shaw.com	UID@domain.com	Wednesday Bonus codes
2014-01-24 8:45	buddy2@email.com		wed codes
2014-01-24 8:47	unknsub@shaw.com	UID@domain.com	FW: Flight(s) Operated By WestJet - LILLIAN LAI
2014-01-24 8:57	unknsub@shaw.com	UID@domain.com	FW: If this doesn't make you smile you you have no heart!!!
2014-01-24 9:42	UID@domain.com	unknsub@shaw.com	RE: Flight(s) Operated By WestJet - LILLIAN LAI
2014-01-24 12:31	ESC1103364926241_1102486473176_1583@in.constantcontact.com	UID@domain.com	News from Canoe Brewpub, Restaurant & Marina
2014-01-24 12:42	erewards@e-rewards.net	UID@domain.com	Profile Update: Mobile Phones

Messages to or from UID@domain.com
Between 0001 and 1245 hrs
2014-Jan-24

date	time	cs-username	cs-method	cs-uri-stem	c-ip
2014-01-24	13:49:55	domain/UID	GET	exchange/UID	76.193.130.252
2014-01-24	13:49:55	domain/UID	GET	exchange/UID/	76.193.130.252
2014-01-24	13:49:56	domain/UID	GET	exchange/UID/	76.193.130.252
2014-01-24	13:49:56	domain/UID	GET	exchange/UID/Inbox/	76.193.130.252
2014-01-24	13:49:56	domain/UID	GET	exchange/UID/	76.193.130.252
2014-01-24	13:49:56	domain/UID	GET	exchange/UID/	76.193.130.252
2014-01-24	13:49:56	domain/UID	GET	exchange/UID/	76.193.130.252
2014-01-24	13:49:56	domain/UID	GET	exchange/UID/	76.193.130.252
2014-01-24	13:49:58	domain/UID	SEARCH	exchange/UID/Inbox/	76.193.130.252
2014-01-24	13:49:58	domain/UID	GET	exchange/UID/Inbox/Looking+for+the+perfect+Mother's+Day+gift_x003F_.EML	76.193.130.252
2014-01-24	13:49:59	domain/UID	SUBSCRIBE	exchange/UID/Calendar	76.193.130.252
2014-01-24	13:49:59	domain/UID	SUBSCRIBE	exchange/UID/Tasks	76.193.130.252
2014-01-24	13:49:59	domain/UID	SEARCH	exchange/UID/Tasks	76.193.130.252
2014-01-24	13:49:59	domain/UID	SEARCH	exchange/UID/Calendar	76.193.130.252
2014-01-24	13:50:08	domain/UID	BPROPPATCH	exchange/UID/	76.193.130.252
2014-01-24	13:50:08	domain/UID	GET	exchange/UID/Inbox/Re:+Sadness+vs+Happiness.EML	76.193.130.252
2014-01-24	13:50:21	domain/UID	BPROPPATCH	exchange/UID/	76.193.130.252
2014-01-24	13:50:22	domain/UID	GET	exchange/UID/Inbox/Re:+Sadness+vs+Happiness-2.EML	76.193.130.252
2014-01-24	13:50:42	domain/UID	PROPFIND	exchange/UID/Sent+Items/	76.193.130.252
2014-01-24	13:50:42	domain/UID	GET	exchange/UID/Sent+Items/	76.193.130.252
2014-01-24	13:50:42	domain/UID	BPROPPATCH	exchange/UID/	76.193.130.252
2014-01-24	13:50:42	domain/UID	SEARCH	exchange/UID/Sent+Items/	76.193.130.252
2014-01-24	13:50:44	domain/UID	GET	exchange/UID/Sent+Items/RE:+Finance+Quotes+++CAMPUS+HONDA.EML	76.193.130.252
2014-01-24	13:50:44	domain/UID	GET	exchange/UID/Sent+Items/RE:+Finance+Quotes+++CAMPUS+HONDA.EML/1_multipart/image001.gif	76.193.130.252
2014-01-24	13:50:48	domain/UID	PROPFIND	exchange/UID/Deleted+Items/	76.193.130.252
2014-01-24	13:50:48	domain/UID	GET	exchange/UID/Deleted+Items/	76.193.130.252
2014-01-24	13:50:48	domain/UID	SEARCH	exchange/UID/Deleted+Items/	76.193.130.252
2014-01-24	13:50:56	domain/UID	SUBSCRIBE	exchange/UID/Inbox	76.193.130.252
2014-01-24	13:51:01	domain/UID	GET	exchange/UID/Deleted+Items/RE:+When+I+win+this,+will+you+come+_x003F_.EML	76.193.130.252
2014-01-24	13:52:37	domain/UID	GET	exchange/UID/Deleted+Items/When+I+win+this,+will+you+come+_x003F_.EML	76.193.130.252

date	time	cs-username	cs-method	cs-uri-stem	c-ip
2014-01-24	13:52:56	domain/UID	GET	exchange/UID/Deleted+Items/Online+statement+notification+from+MBNA+Canada+Bank+re:+Your+Account.EML	76.193.130.252
2014-01-24	13:52:57	domain/UID	POLL	exchange/UID/Inbox	76.193.130.252
2014-01-24	13:53:14	domain/UID	PROPFIND	exchange/UID/Drafts/	76.193.130.252
2014-01-24	13:53:15	domain/UID	GET	exchange/UID/Drafts/	76.193.130.252
2014-01-24	13:53:15	domain/UID	SEARCH	exchange/UID/Drafts/	76.193.130.252
2014-01-24	13:53:16	domain/UID	GET	exchange/UID/Drafts/2+Salad+Dressing+Recipes+from+Island+30's+Mar.+23rd.+show.EML	76.193.130.252
2014-01-24	13:53:19	domain/UID	GET	exchange/UID/Sent+Items/	76.193.130.252
2014-01-24	13:53:19	domain/UID	PROPFIND	exchange/UID/Sent+Items/	76.193.130.252
2014-01-24	13:53:20	domain/UID	SEARCH	exchange/UID/Sent+Items/	76.193.130.252
2014-01-24	13:53:20	domain/UID	GET	exchange/UID/Sent+Items/RE:+Finance+Quotes+++CAMPUS+HONDA.EML	76.193.130.252
2014-01-24	13:53:20	domain/UID	GET	exchange/UID/Sent+Items/RE:+Finance+Quotes+++CAMPUS+HONDA.EML/1_multipart/image001.gif	76.193.130.252
2014-01-24	13:53:39	domain/UID	PROPFIND	exchange/UID/Inbox/	76.193.130.252
2014-01-24	13:53:39	domain/UID	GET	exchange/UID/Inbox/	76.193.130.252
2014-01-24	13:53:39	domain/UID	POLL	exchange/UID/Inbox	76.193.130.252
2014-01-24	13:53:39	domain/UID	SEARCH	exchange/UID/Inbox/	76.193.130.252
2014-01-24	13:53:40	domain/UID	GET	exchange/UID/Inbox/Looking+for+the+perfect+Mother's+Day+gift_x003F_.EML	76.193.130.252
2014-01-24	13:53:49	domain/UID	GET	exchange/UID/Inbox/Re:+Sadness+vs+Happiness-2.EML	76.193.130.252
2014-01-24	13:53:49	domain/UID	GET	exchange/UID/Inbox/Re:+Sadness+vs+Happiness-2.EML	76.193.130.252
2014-01-24	13:54:54	domain/UID	GET	exchange/UID/Inbox/Re:+Sadness+vs+Happiness-2.EML	76.193.130.252
2014-01-24	13:54:54	domain/UID	GET	exchange/UID/Drafts/FW:+Sadness+vs+Happiness.EML	76.193.130.252
2014-01-24	13:54:56	domain/UID	POLL	exchange/UID/Inbox	76.193.130.252
2014-01-24	13:55:11	domain/UID	GET	exchange/UID/Inbox/Thank+you+for+entering+the+Spring+Collection+Contest.EML	76.193.130.252
2014-01-24	13:55:54	domain/UID	GET	exchange/UID/Deleted+Items/	76.193.130.252
2014-01-24	13:55:54	domain/UID	PROPFIND	exchange/UID/Deleted+Items/	76.193.130.252
2014-01-24	13:55:54	domain/UID	SEARCH	exchange/UID/Deleted+Items/	76.193.130.252
2014-01-24	13:56:00	domain/UID	GET	exchange/UID/Deleted+Items/When+I+win+this,+will+you+come+_x003F_.EML	76.193.130.252
2014-01-24	13:56:57	domain/UID	POLL	exchange/UID/Inbox	76.193.130.252

date	time	cs-username	cs-method	cs-uri-stem	c-ip
2014-01-24	13:57:04	domain/UID	POST	exchange/UID/Drafts/FW:+Sadness+vs+Happiness.EML	76.193.130.252
2014-01-24	13:57:11	domain/UID	GET	exchange/UID/Inbox/	76.193.130.252
2014-01-24	13:57:11	domain/UID	PROPFIND	exchange/UID/Inbox/	76.193.130.252
2014-01-24	13:57:11	domain/UID	POLL	exchange/UID/Inbox	76.193.130.252
2014-01-24	13:57:11	domain/UID	SEARCH	exchange/UID/Inbox/	76.193.130.252
2014-01-24	13:57:12	domain/UID	GET	exchange/UID/Inbox/Looking+for+the+perfect+Mother's+Day+gift_x003F_.EML	76.193.130.252
2014-01-24	13:57:13	domain/UID	GET	exchange/UID/Inbox/Re:+Sadness+vs+Happiness.EML	76.193.130.252
2014-01-24	13:57:19	domain/UID	GET	exchange/UID/Inbox/Re:+Sadness+vs+Happiness.EML	76.193.130.252
2014-01-24	13:57:19	domain/UID	GET	exchange/UID/Drafts/FW:+Sadness+vs+Happiness.EML	76.193.130.252
2014-01-24	13:57:47	domain/UID	POST	exchange/UID/Drafts/FW:+Sadness+vs+Happiness.EML	76.193.130.252
2014-01-24	13:57:59	domain/UID	GET	exchange/UID/Sent+Items/	76.193.130.252
2014-01-24	13:57:59	domain/UID	PROPFIND	exchange/UID/Sent+Items/	76.193.130.252
2014-01-24	13:58:01	domain/UID	SEARCH	exchange/UID/Sent+Items/	76.193.130.252
2014-01-24	13:58:01	domain/UID	GET	exchange/UID/Sent+Items/Sadness+vs+Happiness-2.EML	76.193.130.252
2014-01-24	13:58:07	domain/UID	GET	exchange/UID/Sent+Items/Sadness+vs+Happiness-2.EML	76.193.130.252
2014-01-24	13:58:14	domain/UID	BMOVE	exchange/UID/Sent+Items/	76.193.130.252
2014-01-24	13:58:15	domain/UID	GET	exchange/UID/Sent+Items/Sadness+vs+Happiness.EML	76.193.130.252
2014-01-24	13:58:15	domain/UID	BMOVE	exchange/UID/Sent+Items/	76.193.130.252
2014-01-24	13:58:15	domain/UID	SEARCH	exchange/UID/Sent+Items/	76.193.130.252
2014-01-24	13:58:16	domain/UID	GET	exchange/UID/Sent+Items/RE:+Finance+Quotes+++CAMPUS+HONDA.EML	76.193.130.252
2014-01-24	13:58:16	domain/UID	GET	exchange/UID/Sent+Items/RE:+Finance+Quotes+++CAMPUS+HONDA.EML/1_multipart/image001.gif	76.193.130.252
2014-01-24	13:58:18	domain/UID	PROPFIND	exchange/UID/Deleted+Items/	76.193.130.252
2014-01-24	13:58:18	domain/UID	GET	exchange/UID/Deleted+Items/	76.193.130.252
2014-01-24	13:58:18	domain/UID	SEARCH	exchange/UID/Deleted+Items/	76.193.130.252
2014-01-24	13:58:22	domain/UID	BPROPPATCH	exchange/UID/	76.193.130.252
2014-01-24	13:58:22	domain/UID	BDELETE	exchange/UID/Deleted+Items/	76.193.130.252
2014-01-24	13:58:25	domain/UID	BPROPPATCH	exchange/UID/	76.193.130.252
2014-01-24	13:58:25	domain/UID	BDELETE	exchange/UID/Deleted+Items/	76.193.130.252
2014-01-24	13:58:46	domain/UID	GET	exchange/UID/Deleted+Items/	76.193.130.252
2014-01-24	13:58:46	domain/UID	SEARCH	exchange/UID/Deleted+Items/	76.193.130.252

SENG460 Instructor Data

date	time	cs-username	cs-method	cs-uri-stem	c-ip
2014-01-24	13:58:51	domain/UID	BPROPPATCH	exchange/UID/	76.193.130.252
2014-01-24	13:58:51	domain/UID	BDELETE	exchange/UID/Deleted+Items/	76.193.130.252
2014-01-24	13:58:55	domain/UID	BPROPPATCH	exchange/UID/	76.193.130.252
2014-01-24	13:58:55	domain/UID	BDELETE	exchange/UID/Deleted+Items/	76.193.130.252
2014-01-24	13:58:57	domain/UID	POLL	exchange/UID/Inbox	76.193.130.252
2014-01-24	13:58:58	domain/UID	POLL	exchange/UID/Calendar	76.193.130.252
2014-01-24	13:58:58	domain/UID	POLL	exchange/UID/Tasks	76.193.130.252
2014-01-24	13:58:58	domain/UID	SEARCH	exchange/UID/Calendar	76.193.130.252
2014-01-24	13:59:15	domain/UID	BCOPY	exchange/UID/Deleted+Items/	76.193.130.252
2014-01-24	13:59:15	domain/UID	BPROPPATCH	exchange/UID/	76.193.130.252
2014-01-24	13:59:15	domain/UID	SEARCH	exchange/UID/Deleted+Items/	76.193.130.252
2014-01-24	13:59:15	domain/UID	BDELETE	exchange/UID/Deleted+Items/	76.193.130.252
2014-01-24	13:59:19	domain/UID	SEARCH	exchange/UID/Deleted+Items/	76.193.130.252
2014-01-24	13:59:25	domain/UID	GET	exchange/UID/Inbox/	76.193.130.252
2014-01-24	13:59:25	domain/UID	PROPFIND	exchange/UID/Inbox/	76.193.130.252
2014-01-24	13:59:25	domain/UID	POLL	exchange/UID/Inbox	76.193.130.252
2014-01-24	13:59:25	domain/UID	SEARCH	exchange/UID/Inbox/	76.193.130.252
2014-01-24	13:59:25	domain/UID	GET	exchange/UID/Inbox/Looking+for+the+perfect+Mother's+Day+gift_x003F_.EML	76.193.130.252
2014-01-24	13:59:28	domain/UID	GET	exchange/UID/Sent+Items/	76.193.130.252
2014-01-24	13:59:28	domain/UID	PROPFIND	exchange/UID/Sent+Items/	76.193.130.252
2014-01-24	13:59:28	domain/UID	SEARCH	exchange/UID/Sent+Items/	76.193.130.252
2014-01-24	13:59:29	domain/UID	GET	exchange/UID/Sent+Items/RE:+Finance+Quotes+++CAMPUS+HONDA.EML	76.193.130.252
2014-01-24	13:59:29	domain/UID	GET	exchange/UID/Sent+Items/RE:+Finance+Quotes+++CAMPUS+HONDA.EML/1_multipart/image001.gif	76.193.130.252
2014-01-24	13:59:31	domain/UID	GET	exchange/UID/Inbox/	76.193.130.252
2014-01-24	13:59:31	domain/UID	PROPFIND	exchange/UID/Inbox/	76.193.130.252
2014-01-24	13:59:31	domain/UID	POLL	exchange/UID/Inbox	76.193.130.252
2014-01-24	13:59:31	domain/UID	SEARCH	exchange/UID/Inbox/	76.193.130.252
2014-01-24	13:59:32	domain/UID	GET	exchange/UID/Inbox/Looking+for+the+perfect+Mother's+Day+gift_x003F_.EML	76.193.130.252
2014-01-24	13:59:37	domain/UID	GET	exchange/UID/Inbox/Re:+Sadness+vs+Happiness-2.EML	76.193.130.252
2014-01-24	13:59:38	domain/UID	BMOVE	exchange/UID/Inbox/	76.193.130.252
2014-01-24	13:59:38	domain/UID	GET	exchange/UID/Inbox/Luxury+Suite+Package+from+$109+-+72+Hours+Only!.EML	76.193.130.252
2014-01-24	13:59:39	domain/UID	BPROPPATCH	exchange/UID/	76.193.130.252

SENG460 Instructor Data

date	time	cs-username	cs-method	cs-uri-stem	c-ip
2014-01-24	13:59:39	domain/UID	GET	exchange/UID/Inbox/Re:+Sadness+vs+Happiness.EML	76.193.130.252
2014-01-24	13:59:41	domain/UID	BMOVE	exchange/UID/Inbox/	76.193.130.252
2014-01-24	13:59:42	domain/UID	GET	exchange/UID/Inbox/Three+Ways,+One+Place,+Rates+from+$39.EML	76.193.130.252
2014-01-24	13:59:47	domain/UID	PROPFIND	exchange/UID/Deleted+Items/	76.193.130.252
2014-01-24	13:59:47	domain/UID	GET	exchange/UID/Deleted+Items/	76.193.130.252
2014-01-24	13:59:47	domain/UID	BPROPPATCH	exchange/UID/	76.193.130.252
2014-01-24	13:59:47	domain/UID	SEARCH	exchange/UID/Deleted+Items/	76.193.130.252
2014-01-24	13:59:57	domain/UID	GET	exchange/UID/Deleted+Items/RE:+Happy+Tuesday,+Baby.EML	76.193.130.252
2014-01-24	14:00:01	domain/UID	GET	exchange/UID/Deleted+Items/RE:+Happy+Tuesday,+Baby.EML	76.193.130.252
2014-01-24	14:00:01	domain/UID	GET	exchange/UID/Drafts/FW:+Happy+Tuesday,+Baby.EML	76.193.130.252
2014-01-24	14:00:29	domain/UID	POST	exchange/UID/Drafts/FW:+Happy+Tuesday,+Baby.EML	76.193.130.252
2014-01-24	14:00:40	domain/UID	BPROPPATCH	exchange/UID/	76.193.130.252
2014-01-24	14:00:40	domain/UID	BDELETE	exchange/UID/Deleted+Items/	76.193.130.252
2014-01-24	14:00:44	domain/UID	GET	exchange/UID/Deleted+Items/RE:+When+I+win+this,+will+you+come+_x003F_.EML	76.193.130.252
2014-01-24	14:00:50	domain/UID	GET	exchange/UID/Deleted+Items/RE:+When+I+win+this,+will+you+come+_x003F_.EML	76.193.130.252
2014-01-24	14:00:50	domain/UID	GET	exchange/UID/Drafts/FW:+When+I+win+this,+will+you+come+_x003F_.EML	76.193.130.252
2014-01-24	14:00:50	domain/UID	GET	exchange/UID/Drafts/FW:+When+I+win+this,+will+you+come+_x003F_.EML/	76.193.130.252
2014-01-24	14:00:57	domain/UID	POLL	exchange/UID/Inbox	76.193.130.252
2014-01-24	14:01:02	domain/UID	POST	exchange/UID/Drafts/FW:+When+I+win+this,+will+you+come+_x003F_.EML	76.193.130.252
2014-01-24	14:01:11	domain/UID	GET	exchange/UID/Deleted+Items/Re:+Sadness+vs+Happiness-2.EML	76.193.130.252
2014-01-24	14:01:19	domain/UID	GET	exchange/UID/Sent+Items/	76.193.130.252
2014-01-24	14:01:19	domain/UID	PROPFIND	exchange/UID/Sent+Items/	76.193.130.252
2014-01-24	14:01:20	domain/UID	SEARCH	exchange/UID/Sent+Items/	76.193.130.252
2014-01-24	14:01:20	domain/UID	GET	exchange/UID/Sent+Items/FW:+When+I+win+this,+will+you+come+_x003F_.EML	76.193.130.252

SENG460 Instructor Data

date	time	cs-username	cs-method	cs-uri-stem	c-ip
2014-01-24	14:01:20	domain/UID	GET	exchange/UID/Sent+Items/FW:+When+I+win+this,+will+you+come+_x003F_.EML/	76.193.130.252
2014-01-24	14:01:24	domain/UID	BMOVE	exchange/UID/Sent+Items/	76.193.130.252
2014-01-24	14:01:24	domain/UID	GET	exchange/UID/Sent+Items/+Happy+Tuesday,+Baby.EML	76.193.130.252
2014-01-24	14:01:25	domain/UID	BMOVE	exchange/UID/Sent+Items/	76.193.130.252
2014-01-24	14:01:25	domain/UID	SEARCH	exchange/UID/Sent+Items/	76.193.130.252
2014-01-24	14:01:26	domain/UID	GET	exchange/UID/Sent+Items/RE:+Finance+Quotes+++CAMPUS+HONDA.EML	76.193.130.252
2014-01-24	14:01:26	domain/UID	GET	exchange/UID/Sent+Items/RE:+Finance+Quotes+++CAMPUS+HONDA.EML/1_multipart/image001.gif	76.193.130.252
2014-01-24	14:01:27	domain/UID	GET	exchange/UID/Deleted+Items/	76.193.130.252
2014-01-24	14:01:27	domain/UID	PROPFIND	exchange/UID/Deleted+Items/	76.193.130.252
2014-01-24	14:01:27	domain/UID	SEARCH	exchange/UID/Deleted+Items/	76.193.130.252
2014-01-24	14:01:34	domain/UID	BPROPPATCH	exchange/UID/	76.193.130.252
2014-01-24	14:01:34	domain/UID	BDELETE	exchange/UID/Deleted+Items/	76.193.130.252
2014-01-24	14:01:42	domain/UID	BPROPPATCH	exchange/UID/	76.193.130.252
2014-01-24	14:01:42	domain/UID	BDELETE	exchange/UID/Deleted+Items/	76.193.130.252
2014-01-24	14:01:46	domain/UID	BPROPPATCH	exchange/UID/	76.193.130.252
2014-01-24	14:01:46	domain/UID	BDELETE	exchange/UID/Deleted+Items/	76.193.130.252
2014-01-24	14:01:49	domain/UID	BPROPPATCH	exchange/UID/	76.193.130.252
2014-01-24	14:01:49	domain/UID	BDELETE	exchange/UID/Deleted+Items/	76.193.130.252
2014-01-24	14:01:55	domain/UID	GET	exchange/UID/Deleted+Items/	76.193.130.252
2014-01-24	14:01:56	domain/UID	SEARCH	exchange/UID/Deleted+Items/	76.193.130.252
2014-01-24	14:02:22	domain/UID	BPROPPATCH	exchange/UID/	76.193.130.252
2014-01-24	14:02:22	domain/UID	BDELETE	exchange/UID/Deleted+Items/	76.193.130.252
2014-01-24	14:02:33	domain/UID	BPROPPATCH	exchange/UID/	76.193.130.252
2014-01-24	14:02:33	domain/UID	BDELETE	exchange/UID/Deleted+Items/	76.193.130.252
2014-01-24	14:02:55	domain/UID	GET	exchange/UID/Sent+Items/	76.193.130.252
2014-01-24	14:02:55	domain/UID	PROPFIND	exchange/UID/Sent+Items/	76.193.130.252
2014-01-24	14:02:56	domain/UID	SEARCH	exchange/UID/Sent+Items/	76.193.130.252
2014-01-24	14:02:56	domain/UID	GET	exchange/UID/Sent+Items/RE:+Finance+Quotes+++CAMPUS+HONDA.EML	76.193.130.252
2014-01-24	14:02:56	domain/UID	POLL	exchange/UID/Inbox	76.193.130.252

date	time	cs-username	cs-method	cs-uri-stem	c-ip
2014-01-24	14:02:57	domain/UID	GET	exchange/UID/Sent+Items/RE:+Finance+Quotes+++CAMPUS+HONDA.EML/1_multipart/image001.gif	76.193.130.252
2014-01-24	14:02:58	domain/UID	GET	exchange/UID/Inbox/	76.193.130.252
2014-01-24	14:02:58	domain/UID	PROPFIND	exchange/UID/Inbox/	76.193.130.252
2014-01-24	14:02:58	domain/UID	POLL	exchange/UID/Inbox	76.193.130.252
2014-01-24	14:02:58	domain/UID	SEARCH	exchange/UID/Inbox/	76.193.130.252
2014-01-24	14:02:59	domain/UID	GET	exchange/UID/Inbox/Looking+for+the+perfect+Mother's+Day+gift_x003F_.EML	76.193.130.252
2014-01-24	14:03:18	domain/UID	PROPFIND	exchange/UID/Deleted+Items/	76.193.130.252
2014-01-24	14:03:18	domain/UID	GET	exchange/UID/Deleted+Items/	76.193.130.252
2014-01-24	14:03:19	domain/UID	SEARCH	exchange/UID/Deleted+Items/	76.193.130.252
2014-01-24	14:03:26	domain/UID	BPROPPATCH	exchange/UID/	76.193.130.252
2014-01-24	14:03:26	domain/UID	BDELETE	exchange/UID/Deleted+Items/	76.193.130.252
2014-01-24	14:03:32	domain/UID	GET	exchange/UID/Deleted+Items/	76.193.130.252
2014-01-24	14:03:32	domain/UID	SEARCH	exchange/UID/Deleted+Items/	76.193.130.252
2014-01-24	14:03:38	domain/UID	BPROPPATCH	exchange/UID/	76.193.130.252
2014-01-24	14:03:38	domain/UID	BDELETE	exchange/UID/Deleted+Items/	76.193.130.252
2014-01-24	14:03:53	domain/UID	SEARCH	exchange/UID/Deleted+Items/	76.193.130.252
2014-01-24	14:04:18	domain/UID	SEARCH	exchange/UID/Deleted+Items/	76.193.130.252
2014-01-24	14:04:34	domain/UID	SEARCH	exchange/UID/Deleted+Items/	76.193.130.252
2014-01-24	14:04:56	domain/UID	SEARCH	exchange/UID/Deleted+Items/	76.193.130.252
2014-01-24	14:04:57	domain/UID	POLL	exchange/UID/Inbox	76.193.130.252
2014-01-24	14:05:29	domain/UID	SEARCH	exchange/UID/Deleted+Items/	76.193.130.252
2014-01-24	14:06:09	domain/UID	BCOPY	exchange/UID/Deleted+Items/	76.193.130.252
2014-01-24	14:06:09	domain/UID	BPROPPATCH	exchange/UID/	76.193.130.252
2014-01-24	14:06:09	domain/UID	BDELETE	exchange/UID/Deleted+Items/	76.193.130.252
2014-01-24	14:06:09	domain/UID	SEARCH	exchange/UID/Deleted+Items/	76.193.130.252
2014-01-24	14:06:12	domain/UID	SEARCH	exchange/UID/Deleted+Items/	76.193.130.252
2014-01-24	14:06:18	domain/UID	GET	exchange/UID/Deleted+Items/RE:+curious....EML	76.193.130.252
2014-01-24	14:06:27	domain/UID	BPROPPATCH	exchange/UID/	76.193.130.252
2014-01-24	14:06:27	domain/UID	BDELETE	exchange/UID/Deleted+Items/	76.193.130.252
2014-01-24	14:06:36	domain/UID	GET	exchange/UID/Deleted+Items/	76.193.130.252
2014-01-24	14:06:36	domain/UID	SEARCH	exchange/UID/Deleted+Items/	76.193.130.252
2014-01-24	14:06:40	domain/UID	BPROPPATCH	exchange/UID/	76.193.130.252
2014-01-24	14:06:41	domain/UID	BDELETE	exchange/UID/Deleted+Items/	76.193.130.252
2014-01-24	14:06:45	domain/UID	SEARCH	exchange/UID/Deleted+Items/	76.193.130.252
2014-01-24	14:06:56	domain/UID	POLL	exchange/UID/Inbox	76.193.130.252
2014-01-24	14:07:01	domain/UID	SEARCH	exchange/UID/Deleted+Items/	76.193.130.252
2014-01-24	14:07:15	domain/UID	SEARCH	exchange/UID/Deleted+Items/	76.193.130.252

date	time	cs-username	cs-method	cs-uri-stem	c-ip
2014-01-24	14:07:21	domain/UID	SEARCH	exchange/UID/Deleted+Items/	76.193.130.252
2014-01-24	14:07:33	domain/UID	SEARCH	exchange/UID/Deleted+Items/	76.193.130.252
2014-01-24	14:07:58	domain/UID	POLL	exchange/UID/Calendar	76.193.130.252
2014-01-24	14:07:58	domain/UID	POLL	exchange/UID/Tasks	76.193.130.252
2014-01-24	14:08:08	domain/UID	SEARCH	exchange/UID/Deleted+Items/	76.193.130.252
2014-01-24	14:08:13	domain/UID	SEARCH	exchange/UID/Deleted+Items/	76.193.130.252
2014-01-24	14:08:57	domain/UID	POLL	exchange/UID/Inbox	76.193.130.252
2014-01-24	14:08:57	domain/UID	BCOPY	exchange/UID/Deleted+Items/	76.193.130.252
2014-01-24	14:08:57	domain/UID	BPROPPATCH	exchange/UID/	76.193.130.252
2014-01-24	14:08:57	domain/UID	SEARCH	exchange/UID/Deleted+Items/	76.193.130.252
2014-01-24	14:08:57	domain/UID	BDELETE	exchange/UID/Deleted+Items/	76.193.130.252
2014-01-24	14:09:01	domain/UID	SEARCH	exchange/UID/Deleted+Items/	76.193.130.252
2014-01-24	14:09:06	domain/UID	GET	exchange/UID/Deleted+Items/You.EML	76.193.130.252
2014-01-24	14:09:06	domain/UID	GET	exchange/UID/Deleted+Items/You.EML/1_multipart/3_imstp_animation_monkey_en_020908.gif	76.193.130.252
2014-01-24	14:09:07	domain/UID	GET	exchange/UID/Deleted+Items/You.EML/1_multipart/2_image0011.gif	76.193.130.252
2014-01-24	14:09:18	domain/UID	BPROPPATCH	exchange/UID/	76.193.130.252
2014-01-24	14:09:18	domain/UID	BDELETE	exchange/UID/Deleted+Items/	76.193.130.252
2014-01-24	14:09:22	domain/UID	GET	exchange/UID/Deleted+Items/	76.193.130.252
2014-01-24	14:09:23	domain/UID	SEARCH	exchange/UID/Deleted+Items/	76.193.130.252
2014-01-24	14:09:26	domain/UID	BPROPPATCH	exchange/UID/	76.193.130.252
2014-01-24	14:09:26	domain/UID	BDELETE	exchange/UID/Deleted+Items/	76.193.130.252
2014-01-24	14:09:36	domain/UID	SEARCH	exchange/UID/Deleted+Items/	76.193.130.252
2014-01-24	14:09:44	domain/UID	SEARCH	exchange/UID/Deleted+Items/	76.193.130.252
2014-01-24	14:09:55	domain/UID	SEARCH	exchange/UID/Deleted+Items/	76.193.130.252
2014-01-24	14:10:20	domain/UID	SEARCH	exchange/UID/Deleted+Items/	76.193.130.252
2014-01-24	14:10:45	domain/UID	SEARCH	exchange/UID/Deleted+Items/	76.193.130.252
2014-01-24	14:10:56	domain/UID	POLL	exchange/UID/Inbox	76.193.130.252
2014-01-24	14:11:08	domain/UID	SEARCH	exchange/UID/Deleted+Items/	76.193.130.252
2014-01-24	14:11:23	domain/UID	SEARCH	exchange/UID/Deleted+Items/	76.193.130.252
2014-01-24	14:11:46	domain/UID	SEARCH	exchange/UID/Deleted+Items/	76.193.130.252
2014-01-24	14:12:50	domain/UID	PROPFIND	exchange/UID/Sent+Items/	76.193.130.252
2014-01-24	14:12:50	domain/UID	GET	exchange/UID/Sent+Items/	76.193.130.252
2014-01-24	14:12:51	domain/UID	SEARCH	exchange/UID/Sent+Items/	76.193.130.252
2014-01-24	14:12:51	domain/UID	GET	exchange/UID/Sent+Items/RE:+Finance+Quotes+++CAMPUS+HONDA.EML	76.193.130.252

SENG460 Instructor Data

date	time	cs-username	cs-method	cs-uri-stem	c-ip
2014-01-24	14:12:52	domain/UID	GET	exchange/UID/Sent+Items/RE:+Finance+Quotes+++CAMPUS+HONDA.EML/1_multipart/image001.gif	76.193.130.252
2014-01-24	14:12:52	domain/UID	GET	exchange/UID/Deleted+Items/	76.193.130.252
2014-01-24	14:12:53	domain/UID	PROPFIND	exchange/UID/Deleted+Items/	76.193.130.252
2014-01-24	14:12:53	domain/UID	SEARCH	exchange/UID/Deleted+Items/	76.193.130.252
2014-01-24	14:12:56	domain/UID	POLL	exchange/UID/Inbox	76.193.130.252
2014-01-24	14:13:03	domain/UID	GET	exchange/UID/Deleted+Items/	76.193.130.252
2014-01-24	14:13:04	domain/UID	SEARCH	exchange/UID/Deleted+Items/	76.193.130.252
2014-01-24	14:13:35	domain/UID	BCOPY	exchange/UID/Deleted+Items/	76.193.130.252
2014-01-24	14:13:35	domain/UID	SEARCH	exchange/UID/Deleted+Items/	76.193.130.252
2014-01-24	14:13:35	domain/UID	BPROPPATCH	exchange/UID/	76.193.130.252
2014-01-24	14:13:35	domain/UID	BDELETE	exchange/UID/Deleted+Items/	76.193.130.252
2014-01-24	14:13:41	domain/UID	SEARCH	exchange/UID/Deleted+Items/	76.193.130.252
2014-01-24	14:13:46	domain/UID	GET	exchange/UID/Deleted+Items/RE:+Sadness+vs+Happiness.EML	76.193.130.252
2014-01-24	14:13:48	domain/UID	GET	exchange/UID/Deleted+Items/RE:+Sadness+vs+Happiness.EML	76.193.130.252
2014-01-24	14:13:48	domain/UID	GET	exchange/UID/Drafts/FW:+Sadness+vs+Happiness.EML	76.193.130.252
2014-01-24	14:14:01	domain/UID	POST	exchange/UID/Drafts/FW:+Sadness+vs+Happiness.EML	76.193.130.252
2014-01-24	14:14:06	domain/UID	PROPFIND	exchange/UID/Sent+Items/	76.193.130.252
2014-01-24	14:14:07	domain/UID	GET	exchange/UID/Sent+Items/	76.193.130.252
2014-01-24	14:14:07	domain/UID	SEARCH	exchange/UID/Sent+Items/	76.193.130.252
2014-01-24	14:14:07	domain/UID	GET	exchange/UID/Sent+Items/FW:+Sadness+vs+Happiness.EML	76.193.130.252
2014-01-24	14:14:09	domain/UID	BMOVE	exchange/UID/Sent+Items/	76.193.130.252
2014-01-24	14:14:10	domain/UID	GET	exchange/UID/Sent+Items/RE:+Finance+Quotes+++CAMPUS+HONDA.EML	76.193.130.252
2014-01-24	14:14:10	domain/UID	GET	exchange/UID/Sent+Items/RE:+Finance+Quotes+++CAMPUS+HONDA.EML/1_multipart/image001.gif	76.193.130.252
2014-01-24	14:14:13	domain/UID	GET	exchange/UID/Deleted+Items/	76.193.130.252
2014-01-24	14:14:13	domain/UID	PROPFIND	exchange/UID/Deleted+Items/	76.193.130.252
2014-01-24	14:14:13	domain/UID	SEARCH	exchange/UID/Deleted+Items/	76.193.130.252
2014-01-24	14:14:25	domain/UID	BPROPPATCH	exchange/UID/	76.193.130.252
2014-01-24	14:14:25	domain/UID	BDELETE	exchange/UID/Deleted+Items/	76.193.130.252
2014-01-24	14:14:29	domain/UID	GET	exchange/UID/Deleted+Items/	76.193.130.252

SENG460 Instructor Data

date	time	cs-username	cs-method	cs-uri-stem	c-ip
2014-01-24	14:14:29	domain/UID	SEARCH	exchange/UID/Deleted+Items/	76.193.130.252
2014-01-24	14:14:41	domain/UID	BPROPPATCH	exchange/UID/	76.193.130.252
2014-01-24	14:14:41	domain/UID	BDELETE	exchange/UID/Deleted+Items/	76.193.130.252
2014-01-24	14:14:52	domain/UID	SEARCH	exchange/UID/Deleted+Items/	76.193.130.252
2014-01-24	14:14:53	domain/UID	SEARCH	exchange/UID/Deleted+Items/	76.193.130.252
2014-01-24	14:14:55	domain/UID	SEARCH	exchange/UID/Deleted+Items/	76.193.130.252
2014-01-24	14:14:56	domain/UID	SEARCH	exchange/UID/Deleted+Items/	76.193.130.252
2014-01-24	14:14:57	domain/UID	POLL	exchange/UID/Inbox	76.193.130.252
2014-01-24	14:15:03	domain/UID	SEARCH	exchange/UID/Deleted+Items/	76.193.130.252
2014-01-24	14:15:10	domain/UID	SEARCH	exchange/UID/Deleted+Items/	76.193.130.252
2014-01-24	14:15:38	domain/UID	SEARCH	exchange/UID/Deleted+Items/	76.193.130.252
2014-01-24	14:15:46	domain/UID	SEARCH	exchange/UID/Deleted+Items/	76.193.130.252
2014-01-24	14:15:59	domain/UID	SEARCH	exchange/UID/Deleted+Items/	76.193.130.252
2014-01-24	14:16:27	domain/UID	GET	exchange/UID/	76.193.130.252
2014-01-24	14:16:27	domain/UID	GET	/exchweb/bin/USA/logoff.asp	76.193.130.252
2014-01-24	14:16:27	domain/UID	GET	/exchweb/bin/USA/logo_Domain.gif	76.193.130.252