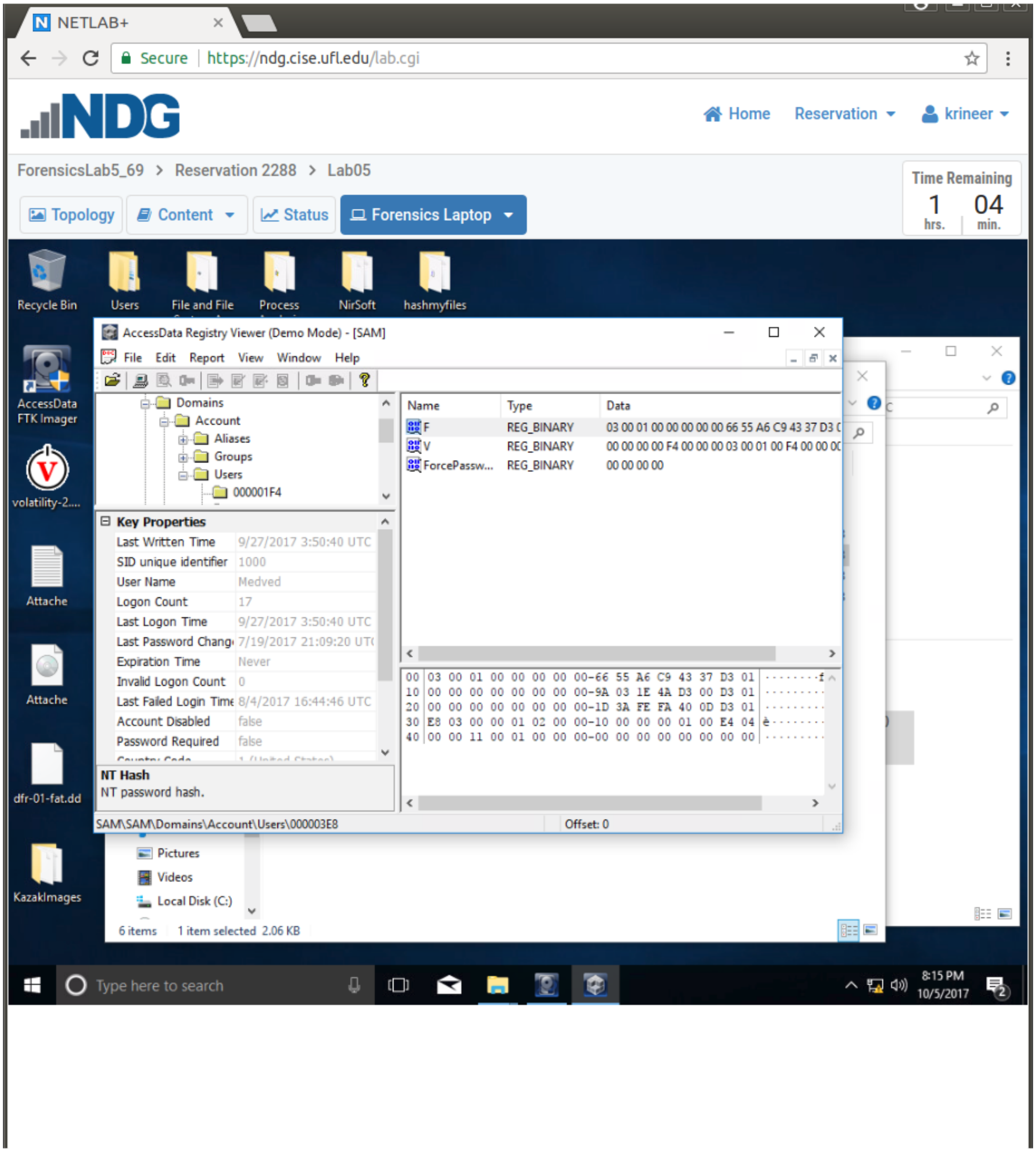
Lab 5 Report
Kevin Rineer
27 Sept 2017

User 000003E8 Name/Full name: Medved
SID of the Medved Account: 1000
Last time Medved logged in: 9/27/2017 3:50:40 UTC
Current Control Set for this Machine: 001
Computer Name for this Machine: KAZAK
NTFSDisableLastAccessUpdate value: 1(True)
TimeZoneInformation: Eastern Standard Time
DHCPIPAddress values: 172.16.28.134
Last shutdown time: 9/27/2017 3:09:34 AM
Windows Product Name: Windows 10 Education
Windows Install Date: Tue Sep 26 23:14:07 2017
Maude Wifi 2.4G DefaultGatewayMac: 76 54 7D F9 72 AF
Maude Wifi 5G DefaultGatewayMac: 76 54 7D F9 72 AF
Maude Wifi 2.4G DateLastConnected:
DCODE: Not a Valid Date
RFV Timestamp 64: 7/28/1604 8:24:21 PM
Maude Wifi 5G DateLastConnected:
DCODE: Not a Valid Date
RFV Timestamp 64: 7/28/1604 8:24:21 PM

Screenshots of relevant information below, though they represent the same data as the list above.



Name	Type	Data
F	REG_BINARY	03 00 01 00 00 00 00 00 66 55 A6 C9 43 37 D3 (
V	REG_BINARY	00 00 00 00 F4 00 00 00 03 00 01 00 F4 00 00 0(
ForcePassw...	REG_BINARY	00 00 00 00

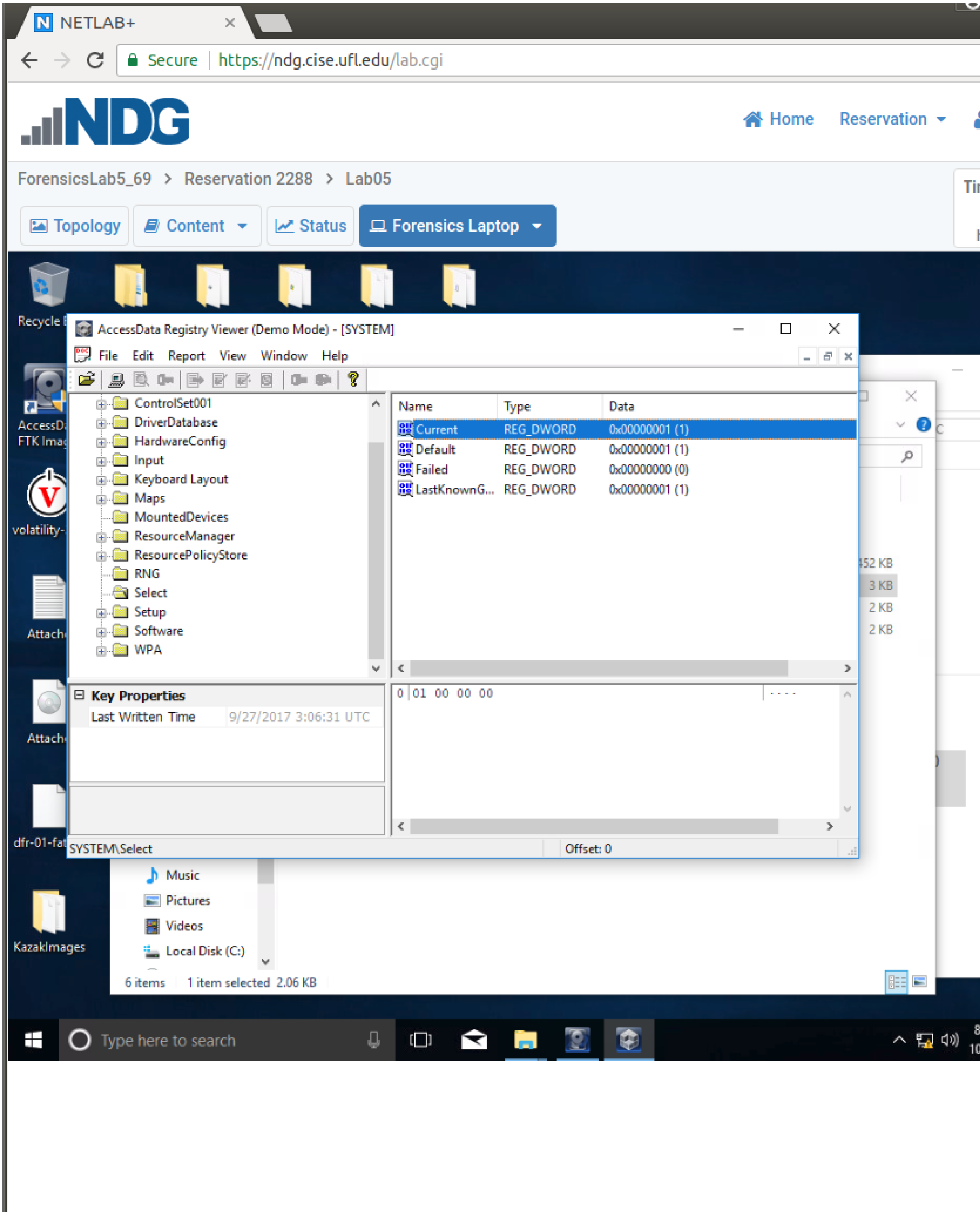
Key Properties	
Last Written Time	9/27/2017 3:50:40 UTC
SID unique identifier	1000
User Name	Medved
Logon Count	17
Last Logon Time	9/27/2017 3:50:40 UTC
Last Password Chang	7/19/2017 21:09:20 UT(
Expiration Time	Never
Invalid Logon Count	0
Last Failed Login Time	8/4/2017 16:44:46 UTC
Account Disabled	false
Password Required	false

```
00 03 00 01 00 00 00 00 00-66 55 A6 C9 43 37 D3 01  ········f
10 00 00 00 00 00 00 00 00-9A 03 1E 4A D3 00 D3 01  ·········
20 00 00 00 00 00 00 00 00-1D 3A FE FA 40 0D D3 01  ·········
30 E8 03 00 00 01 02 00 00-10 00 00 00 01 00 E4 04  è········
40 00 00 11 00 01 00 00 00-00 00 00 00 00 00 00 00  ·········
```

NT Hash

NT password hash.

SAM\SAM\Domains\Account\Users\000003E8   Offset: 0



```
ControlSet001
DriverDatabase
HardwareConfig
Input
Keyboard Layout
Maps
MountedDevices
ResourceManager
ResourcePolicyStore
RNG
Select
Setup
Software
WPA
```

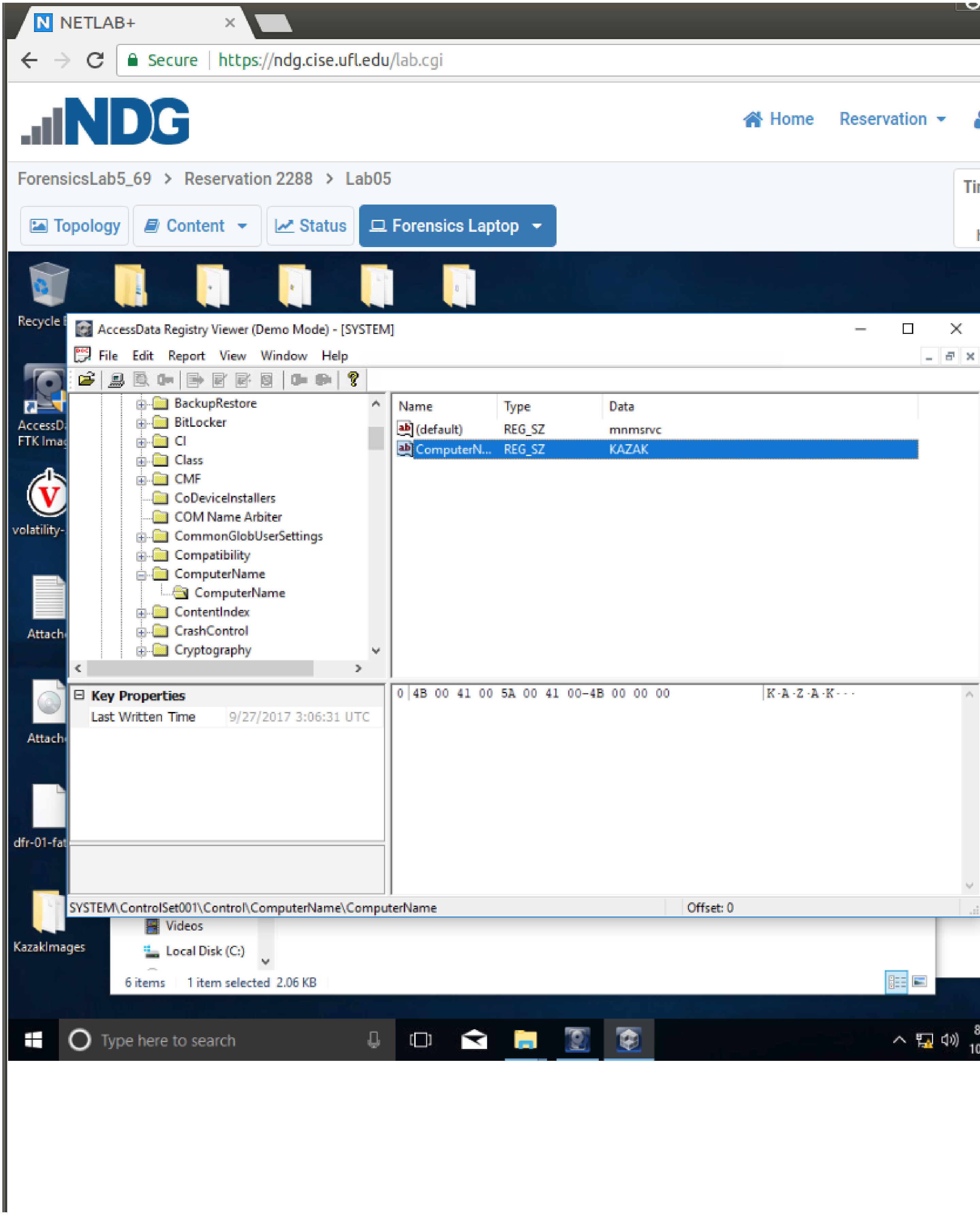
Name	Type	Data
Current	REG_DWORD	0x00000001 (1)
Default	REG_DWORD	0x00000001 (1)
Failed	REG_DWORD	0x00000000 (0)
LastKnownG...	REG_DWORD	0x00000001 (1)

Key Properties

Last Written Time	9/27/2017 3:06:31 UTC

```
0 01 00 00 00    ....
```

SYSTEM\Select   Offset: 0



AccessData Registry Viewer (Demo Mode) - [SYSTEM]

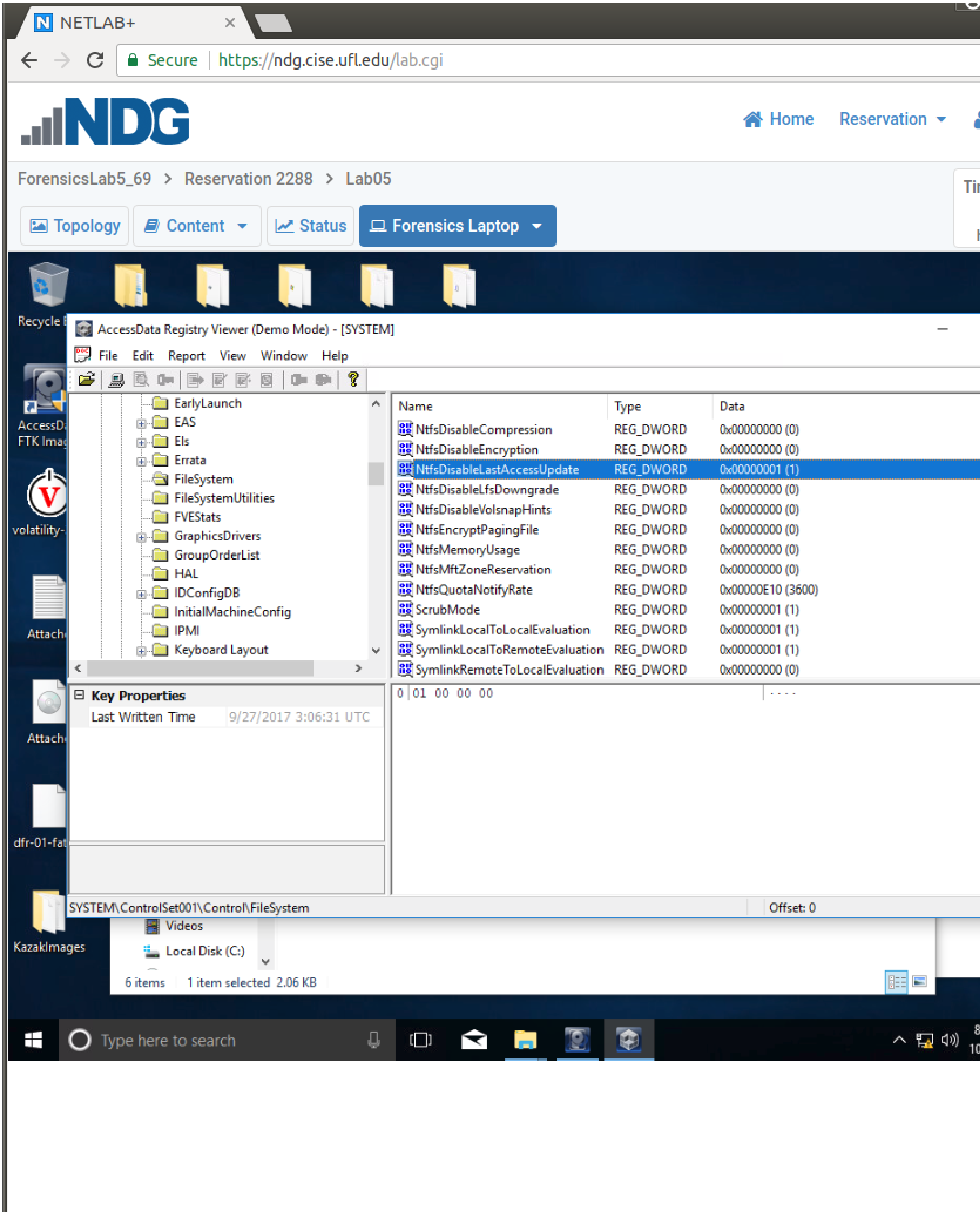
Name	Type	Data
(default)	REG_SZ	mnmsrvc
ComputerN...	REG_SZ	KAZAK

Key Properties

Last Written Time	9/27/2017 3:06:31 UTC

```
0  4B 00 41 00 5A 00 41 00-4B 00 00 00          K·A·Z·A·K···
```

SYSTEM\ControlSet001\Control\ComputerName\ComputerName   Offset: 0



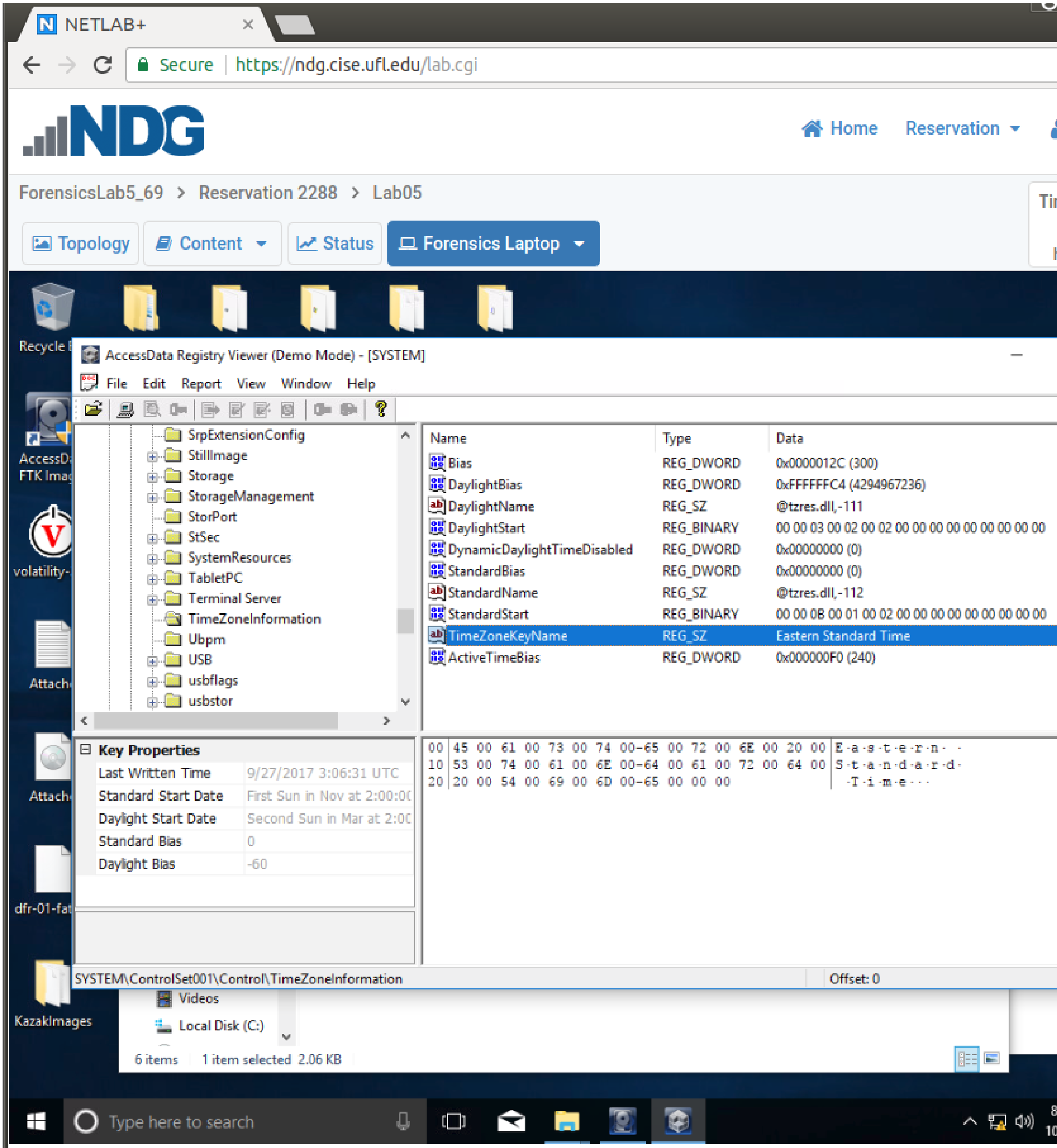
Name	Type	Data
NtfsDisableCompression	REG_DWORD	0x00000000 (0)
NtfsDisableEncryption	REG_DWORD	0x00000000 (0)
NtfsDisableLastAccessUpdate	REG_DWORD	0x00000001 (1)
NtfsDisableLfsDowngrade	REG_DWORD	0x00000000 (0)
NtfsDisableVolsnapHints	REG_DWORD	0x00000000 (0)
NtfsEncryptPagingFile	REG_DWORD	0x00000000 (0)
NtfsMemoryUsage	REG_DWORD	0x00000000 (0)
NtfsMftZoneReservation	REG_DWORD	0x00000000 (0)
NtfsQuotaNotifyRate	REG_DWORD	0x00000E10 (3600)
ScrubMode	REG_DWORD	0x00000001 (1)
SymlinkLocalToLocalEvaluation	REG_DWORD	0x00000001 (1)
SymlinkLocalToRemoteEvaluation	REG_DWORD	0x00000001 (1)
SymlinkRemoteToLocalEvaluation	REG_DWORD	0x00000000 (0)

```
0 01 00 00 00    ....
```

Key Properties

Last Written Time	9/27/2017 3:06:31 UTC

SYSTEM\ControlSet001\Control\FileSystem   Offset: 0

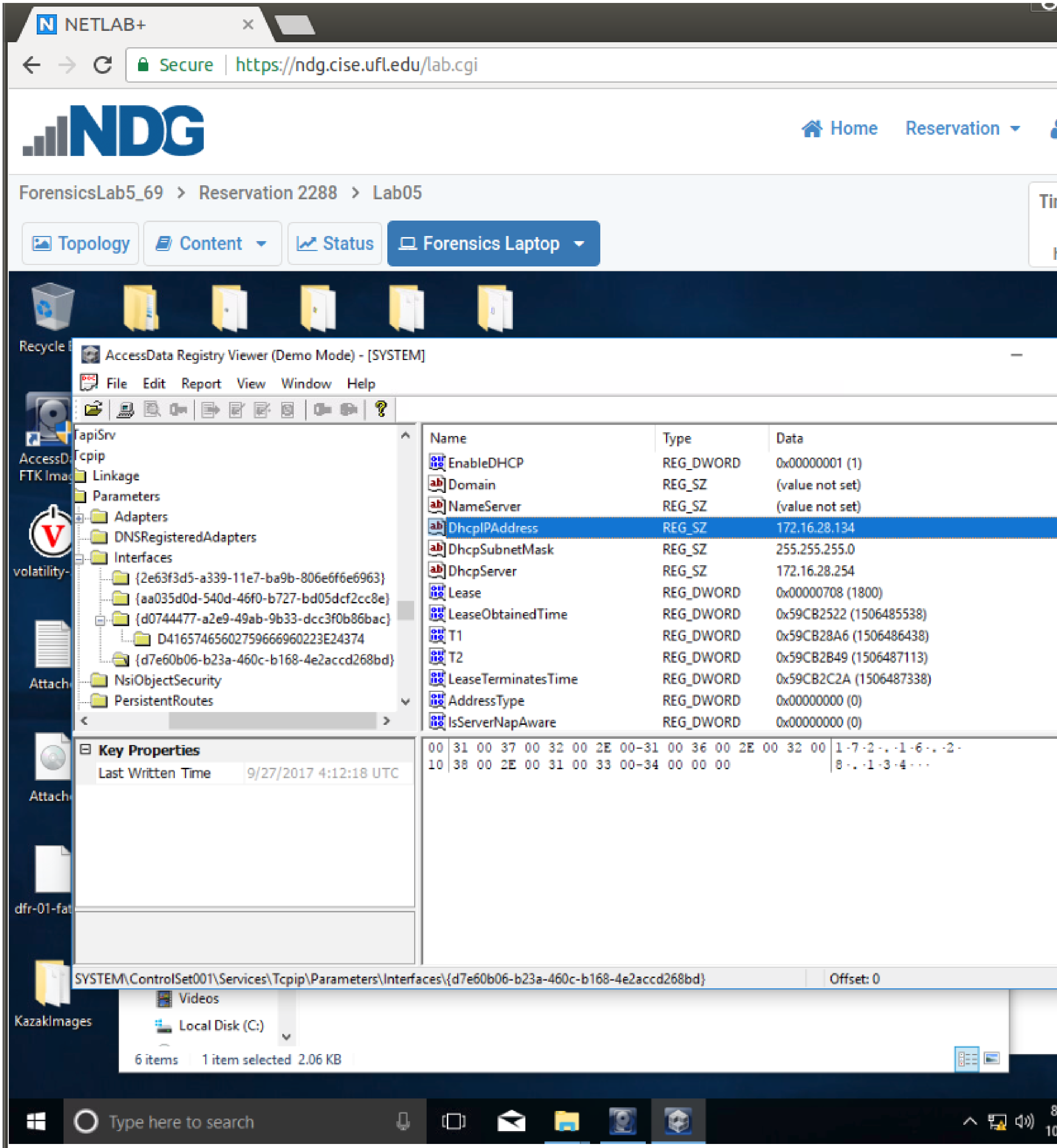


Name	Type	Data
Bias	REG_DWORD	0x0000012C (300)
DaylightBias	REG_DWORD	0xFFFFFFC4 (4294967236)
DaylightName	REG_SZ	@tzres.dll,-111
DaylightStart	REG_BINARY	00 00 03 00 02 00 02 00 00 00 00 00 00 00 00 00
DynamicDaylightTimeDisabled	REG_DWORD	0x00000000 (0)
StandardBias	REG_DWORD	0x00000000 (0)
StandardName	REG_SZ	@tzres.dll,-112
StandardStart	REG_BINARY	00 00 0B 00 01 00 02 00 00 00 00 00 00 00 00 00
TimeZoneKeyName	REG_SZ	Eastern Standard Time
ActiveTimeBias	REG_DWORD	0x000000F0 (240)

Key Properties	
Last Written Time	9/27/2017 3:06:31 UTC
Standard Start Date	First Sun in Nov at 2:00:0
Daylight Start Date	Second Sun in Mar at 2:0
Standard Bias	0
Daylight Bias	-60

```
00 45 00 61 00 73 00 74 00-65 00 72 00 6E 00 20 00  E·a·s·t·e·r·n· ·
10 53 00 74 00 61 00 6E 00-64 00 61 00 72 00 64 00  S·t·a·n·d·a·r·d·
20 20 00 54 00 69 00 6D 00-65 00 00 00               ·T·i·m·e···
```

SYSTEM\ControlSet001\Control\TimeZoneInformation   Offset: 0



NETLAB+
https://ndg.cise.ufl.edu/lab.cgi
Home
Reservation
ForensicsLab5_69 > Reservation 2288 > Lab05
Topology
Content
Status
Forensics Laptop
AccessData Registry Viewer (Demo Mode) - [SYSTEM]
File Edit Report View Window Help

TapiSrv
Tcpip
Linkage
Parameters
Adapters
DNSRegisteredAdapters
Interfaces
{2e63f3d5-a339-11e7-ba9b-806e6f6e6963}
{aa035d0d-540d-46f0-b727-bd05dcf2cc8e}
{d0744477-a2e9-49ab-9b33-dcc3f0b86bac}
D416574656027596669602 23E24374
{d7e60b06-b23a-460c-b168-4e2accd268bd}
NsiObjectSecurity
PersistentRoutes

Name	Type	Data
EnableDHCP	REG_DWORD	0x00000001 (1)
Domain	REG_SZ	(value not set)
NameServer	REG_SZ	(value not set)
DhcpIPAddress	REG_SZ	172.16.28.134
DhcpSubnetMask	REG_SZ	255.255.255.0
DhcpServer	REG_SZ	172.16.28.254
Lease	REG_DWORD	0x00000708 (1800)
LeaseObtainedTime	REG_DWORD	0x59CB2522 (1506485538)
T1	REG_DWORD	0x59CB28A6 (1506486438)
T2	REG_DWORD	0x59CB2B49 (1506487113)
LeaseTerminatesTime	REG_DWORD	0x59CB2C2A (1506487338)
AddressType	REG_DWORD	0x00000000 (0)
IsServerNapAware	REG_DWORD	0x00000000 (0)

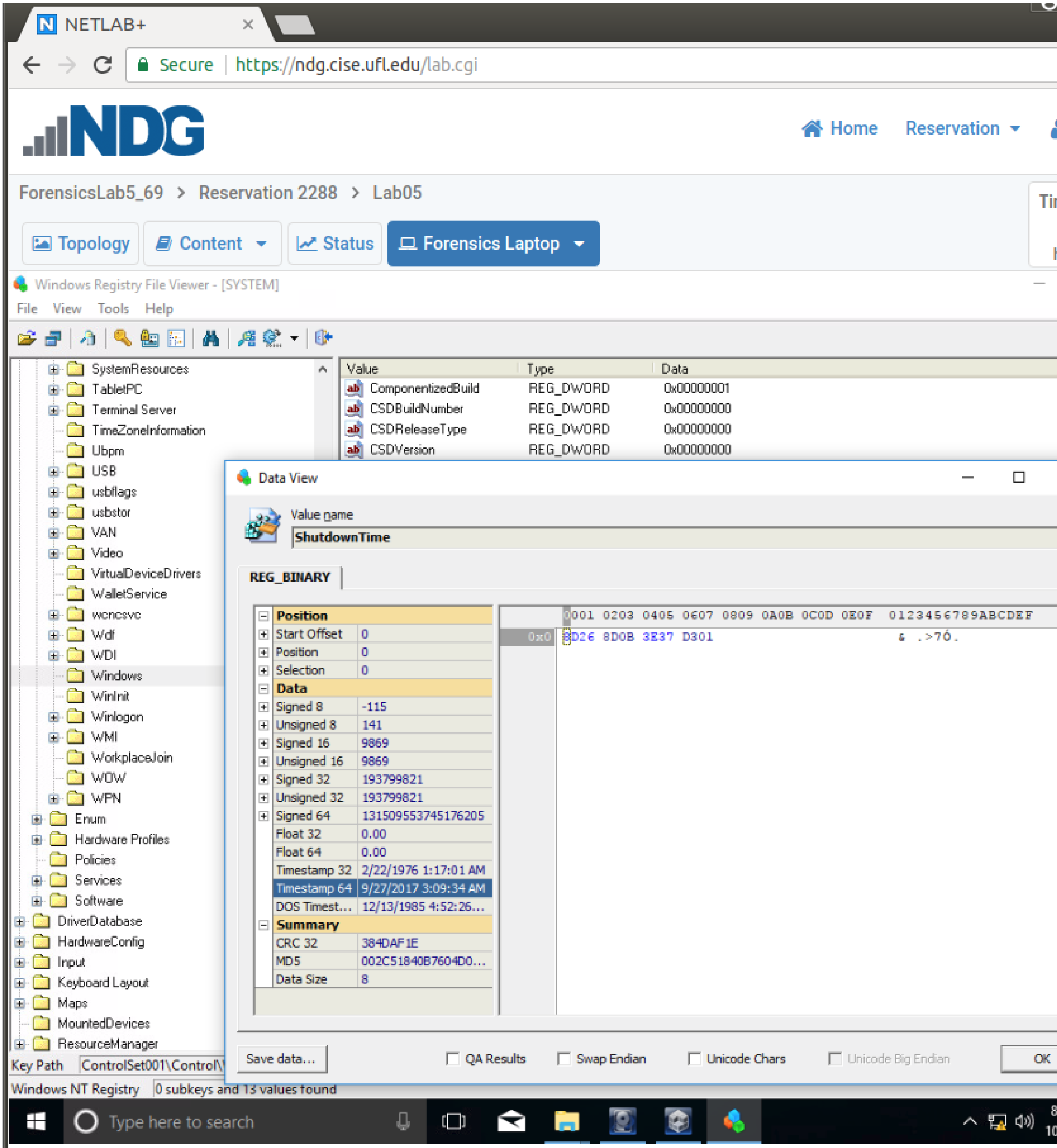
Key Properties

Last Written Time 9/27/2017 4:12:18 UTC

```
00 31 00 37 00 32 00 2E 00-31 00 36 00 2E 00 32 00 |1·7·2·.·1·6·.·2·
10 38 00 2E 00 31 00 33 00-34 00 00 00             |8·.·1·3·4···
```

SYSTEM\ControlSet001\Services\Tcpip\Parameters\Interfaces\{d7e60b06-b23a-460c-b168-4e2accd268bd}   Offset: 0

Lab 5 Report
Kevin Rineer
27 Sept 2017



Value	Type	Data
ComponentizedBuild	REG_DWORD	0x00000001
CSDBuildNumber	REG_DWORD	0x00000000
CSDReleaseType	REG_DWORD	0x00000000
CSDVersion	REG_DWORD	0x00000000

Value name: ShutdownTime

REG_BINARY

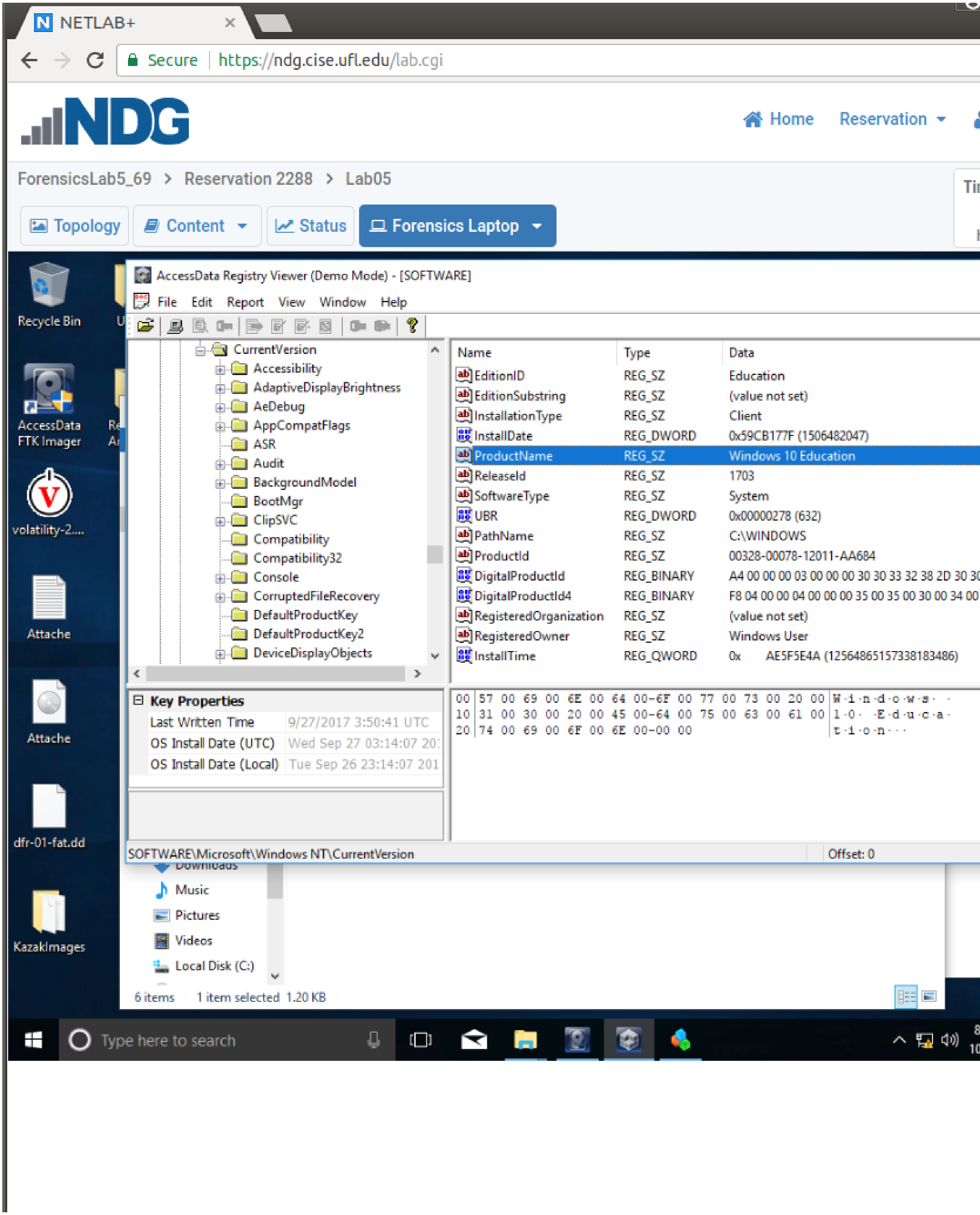
Position	
Start Offset	0
Position	0
Selection	0
Data	
Signed 8	-115
Unsigned 8	141
Signed 16	9869
Unsigned 16	9869
Signed 32	193799821
Unsigned 32	193799821
Signed 64	131509553745176205
Float 32	0.00
Float 64	0.00
Timestamp 32	2/22/1976 1:17:01 AM
Timestamp 64	9/27/2017 3:09:34 AM
DOS Timest...	12/13/1985 4:52:26...
Summary	
CRC 32	384DAF1E
MD5	002C51840B7604D0...
Data Size	8

```
     0001 0203 0405 0607 0809 0A0B 0C0D 0E0F  0123456789ABCDEF
0x0  8D26 8D0B 3E37 D301                      & .>7Ó.
```

□ QA Results □ Swap Endian □ Unicode Chars □ Unicode Big Endian

Key Path: ControlSet001\Control\

Windows NT Registry: 0 subkeys and 13 values found



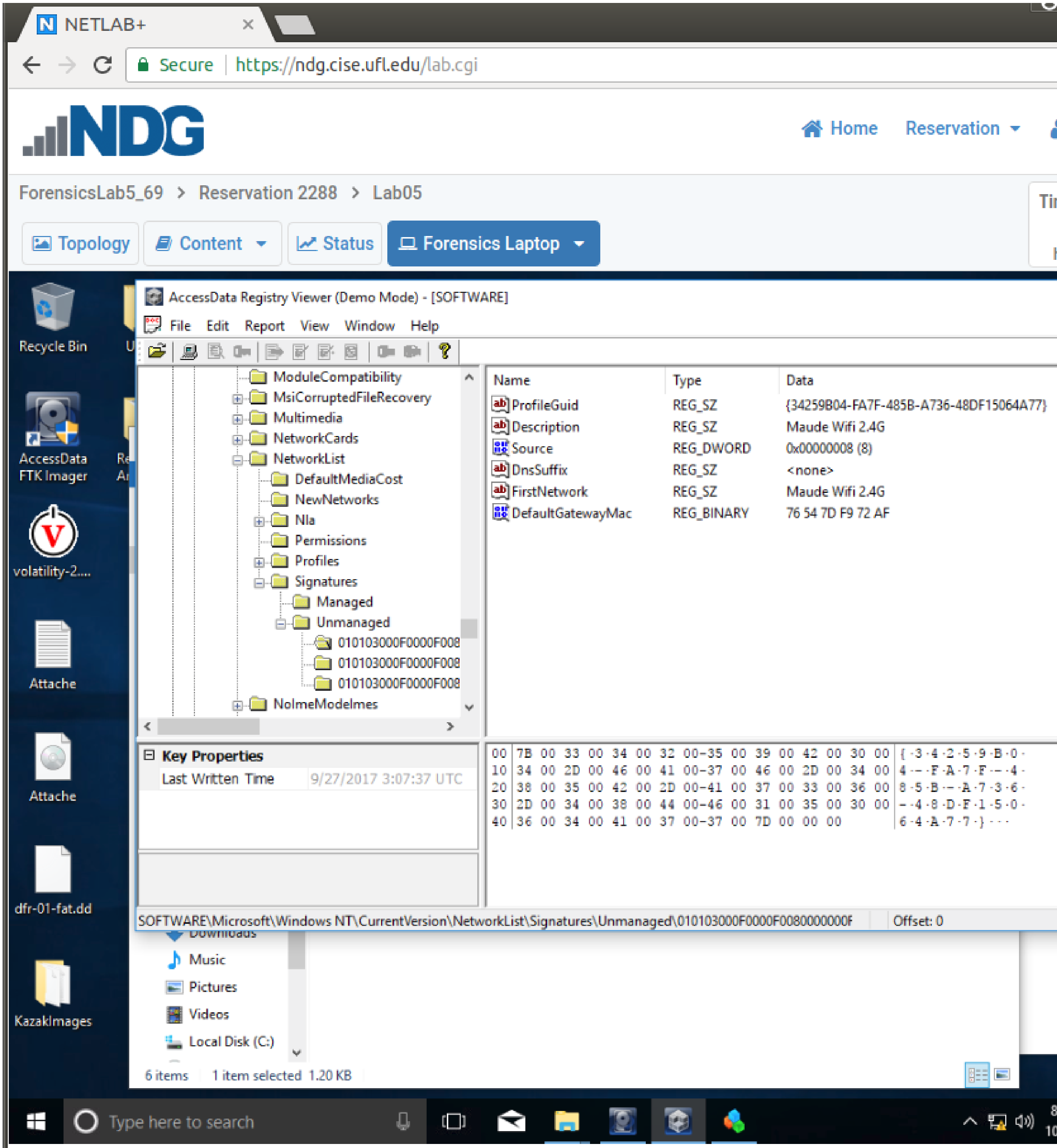
Name	Type	Data
EditionID	REG_SZ	Education
EditionSubstring	REG_SZ	(value not set)
InstallationType	REG_SZ	Client
InstallDate	REG_DWORD	0x59CB177F (1506482047)
ProductName	REG_SZ	Windows 10 Education
ReleaseId	REG_SZ	1703
SoftwareType	REG_SZ	System
UBR	REG_DWORD	0x00000278 (632)
PathName	REG_SZ	C:\WINDOWS
ProductId	REG_SZ	00328-00078-12011-AA684
DigitalProductId	REG_BINARY	A4 00 00 00 03 00 00 00 30 30 33 32 38 2D 30 30
DigitalProductId4	REG_BINARY	F8 04 00 00 04 00 00 00 35 00 35 00 30 00 34 00
RegisteredOrganization	REG_SZ	(value not set)
RegisteredOwner	REG_SZ	Windows User
InstallTime	REG_QWORD	0x AE5F5E4A (12564865157338183486)

```
00  57 00 69 00 6E 00 64 00-6F 00 77 00 73 00 20 00  W·i·n·d·o·w·s·  ·
10  31 00 30 00 20 00 45 00-64 00 75 00 63 00 61 00  1·0·  ·E·d·u·c·a·
20  74 00 69 00 6F 00 6E 00-00 00                    t·i·o·n···
```

Key Properties

Last Written Time	9/27/2017 3:50:41 UTC
OS Install Date (UTC)	Wed Sep 27 03:14:07 20:
OS Install Date (Local)	Tue Sep 26 23:14:07 201

SOFTWARE\Microsoft\Windows NT\CurrentVersion   Offset: 0



AccessData Registry Viewer (Demo Mode) - [SOFTWARE]

Name	Type	Data
ProfileGuid	REG_SZ	{34259B04-FA7F-485B-A736-48DF15064A77}
Description	REG_SZ	Maude Wifi 2.4G
Source	REG_DWORD	0x00000008 (8)
DnsSuffix	REG_SZ	<none>
FirstNetwork	REG_SZ	Maude Wifi 2.4G
DefaultGatewayMac	REG_BINARY	76 54 7D F9 72 AF

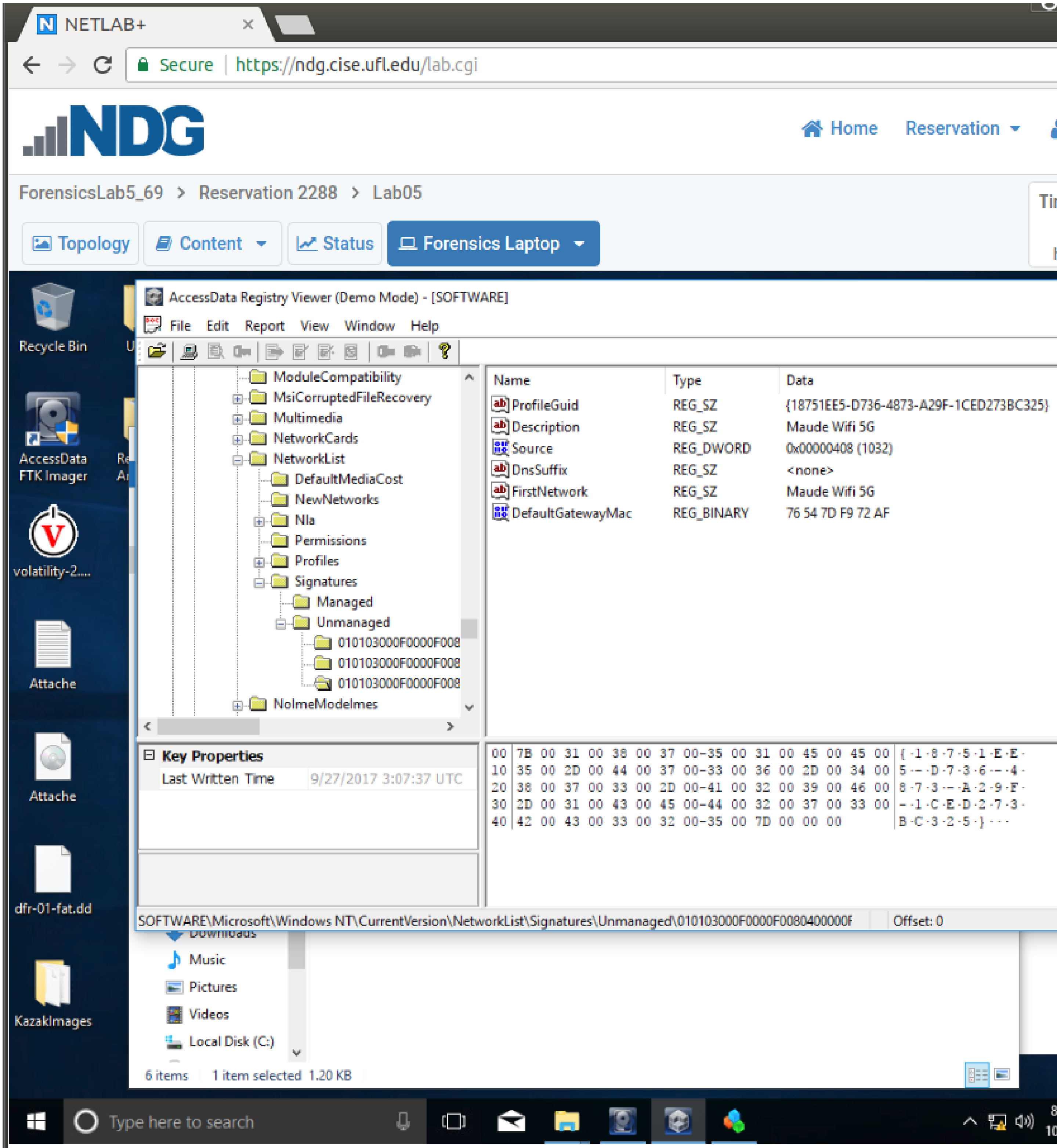
Key Properties

Last Written Time	9/27/2017 3:07:37 UTC

```
00 | 7B 00 33 00 34 00 32 00-35 00 39 00 42 00 30 00 | {·3·4·2·5·9·B·0·
10 | 34 00 2D 00 46 00 41 00-37 00 46 00 2D 00 34 00 | 4·-·F·A·7·F·-·4·
20 | 38 00 35 00 42 00 2D 00-41 00 37 00 33 00 36 00 | 8·5·B·-·A·7·3·6·
30 | 2D 00 34 00 38 00 44 00-46 00 31 00 35 00 30 00 | -·4·8·D·F·1·5·0·
40 | 36 00 34 00 41 00 37 00-37 00 7D 00 00 00       | 6·4·A·7·7·}···
```

SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Signatures\Unmanaged\010103000F0000F0080000000F   Offset: 0

Lab 5 Report
Kevin Rineer
27 Sept 2017



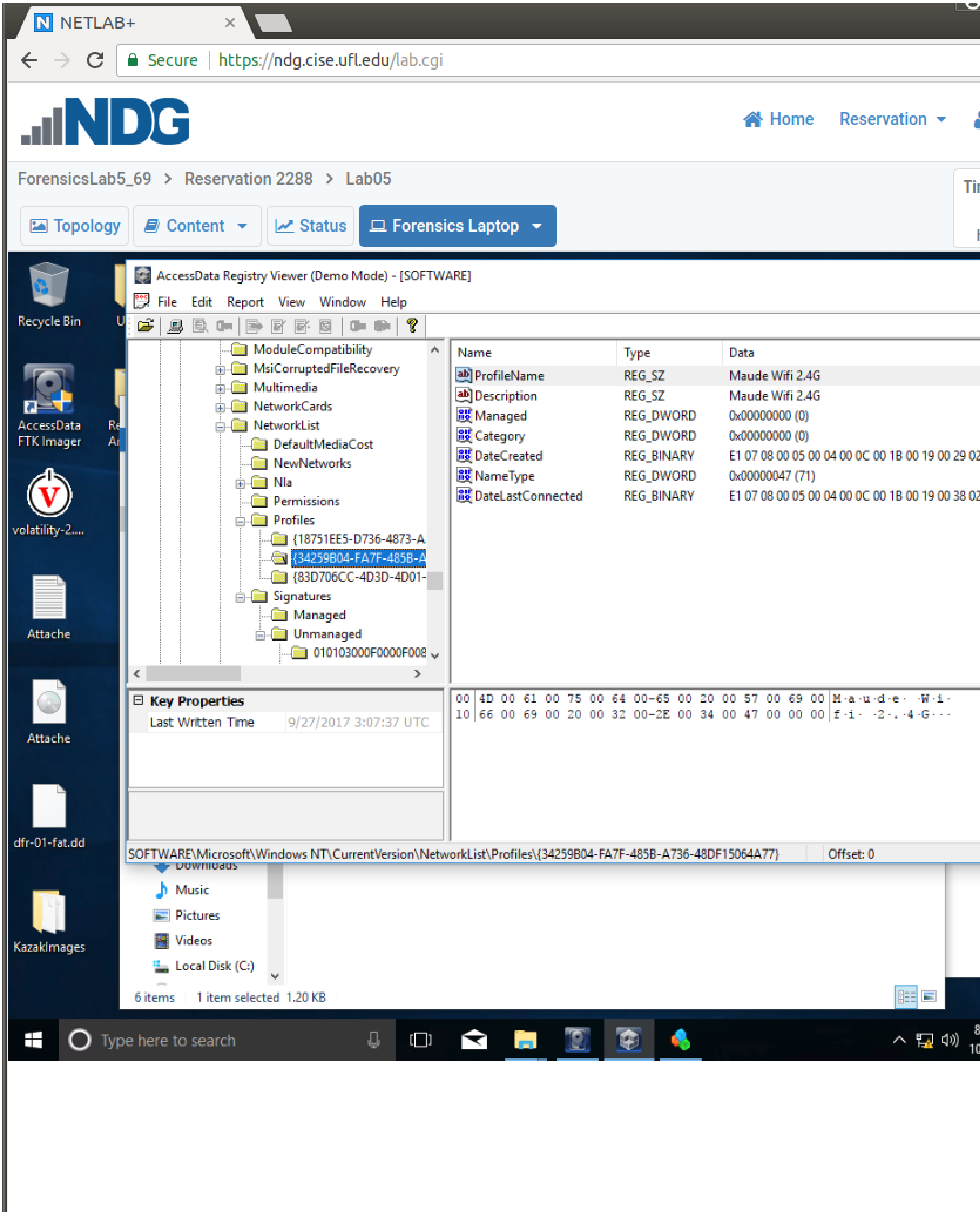
Name	Type	Data
ProfileGuid	REG_SZ	{18751EE5-D736-4873-A29F-1CED273BC325}
Description	REG_SZ	Maude Wifi 5G
Source	REG_DWORD	0x00000408 (1032)
DnsSuffix	REG_SZ	<none>
FirstNetwork	REG_SZ	Maude Wifi 5G
DefaultGatewayMac	REG_BINARY	76 54 7D F9 72 AF

Key Properties

Last Written Time	9/27/2017 3:07:37 UTC

```
00 | 7B 00 31 00 38 00 37 00-35 00 31 00 45 00 45 00 | {·1·8·7·5·1·E·E·
10 | 35 00 2D 00 44 00 37 00-33 00 36 00 2D 00 34 00 | 5·-·D·7·3·6·-·4·
20 | 38 00 37 00 33 00 2D 00-41 00 32 00 39 00 46 00 | 8·7·3·-·A·2·9·F·
30 | 2D 00 31 00 43 00 45 00-44 00 32 00 37 00 33 00 | -·1·C·E·D·2·7·3·
40 | 42 00 43 00 33 00 32 00-35 00 7D 00 00 00       | B·C·3·2·5·}···
```

SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Signatures\Unmanaged\010103000F0000F0080400000F   Offset: 0



AccessData Registry Viewer (Demo Mode) - [SOFTWARE]

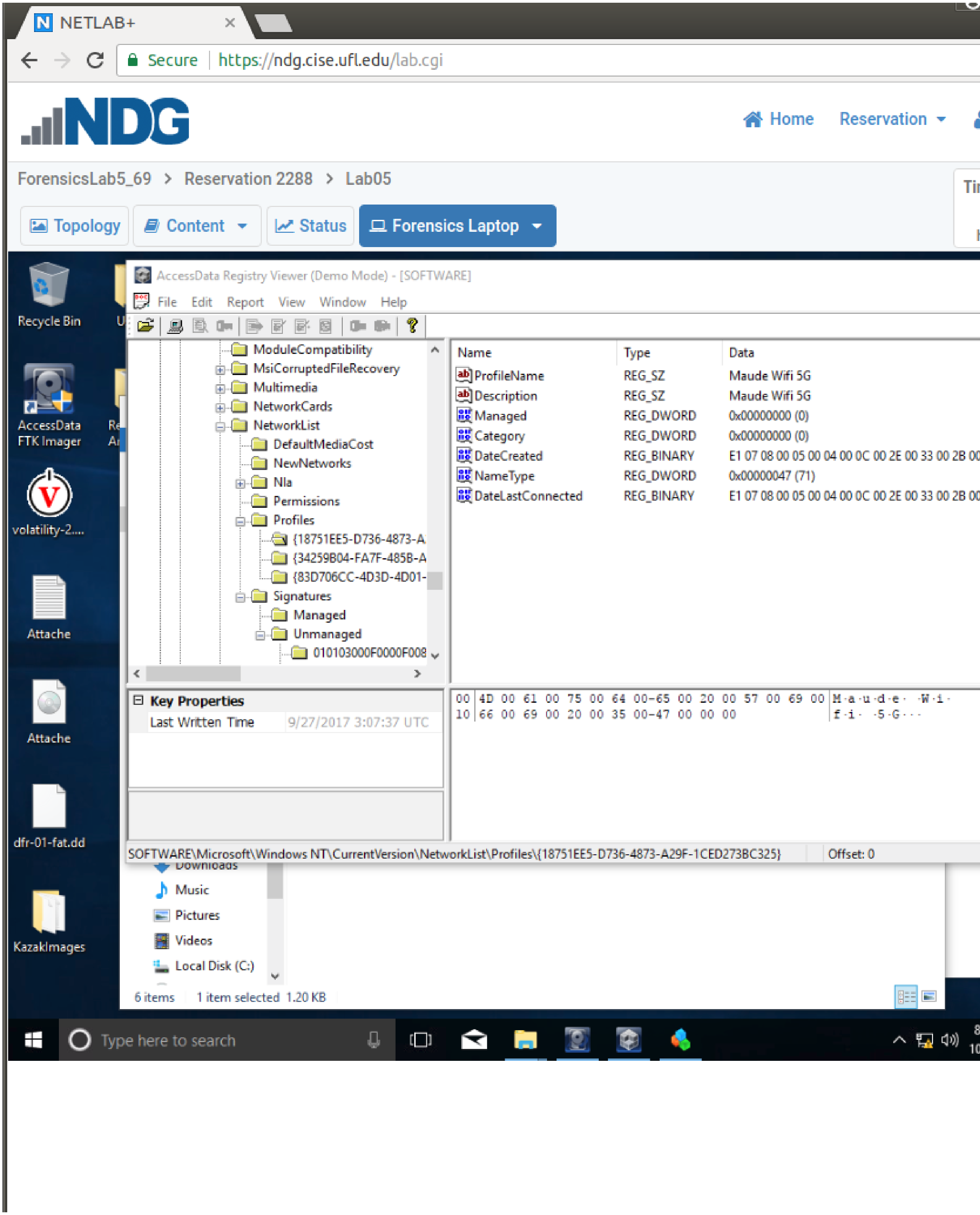
```
ModuleCompatibility
MsiCorruptedFileRecovery
Multimedia
NetworkCards
NetworkList
    DefaultMediaCost
    NewNetworks
    Nla
    Permissions
    Profiles
        {18751EE5-D736-4873-A
        {34259B04-FA7F-485B-A
        {83D706CC-4D3D-4D01-
    Signatures
        Managed
        Unmanaged
            010103000F0000F008
```

Name	Type	Data
ProfileName	REG_SZ	Maude Wifi 2.4G
Description	REG_SZ	Maude Wifi 2.4G
Managed	REG_DWORD	0x00000000 (0)
Category	REG_DWORD	0x00000000 (0)
DateCreated	REG_BINARY	E1 07 08 00 05 00 04 00 0C 00 1B 00 19 00 29 02
NameType	REG_DWORD	0x00000047 (71)
DateLastConnected	REG_BINARY	E1 07 08 00 05 00 04 00 0C 00 1B 00 19 00 38 02

```
00 4D 00 61 00 75 00 64 00-65 00 20 00 57 00 69 00 M·a·u·d·e· ·W·i·
10 66 00 69 00 20 00 32 00-2E 00 34 00 47 00 00 00 f·i· ·2·.·4·G···
```

Key Properties	
Last Written Time	9/27/2017 3:07:37 UTC

SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Profiles\{34259B04-FA7F-485B-A736-48DF15064A77} Offset: 0



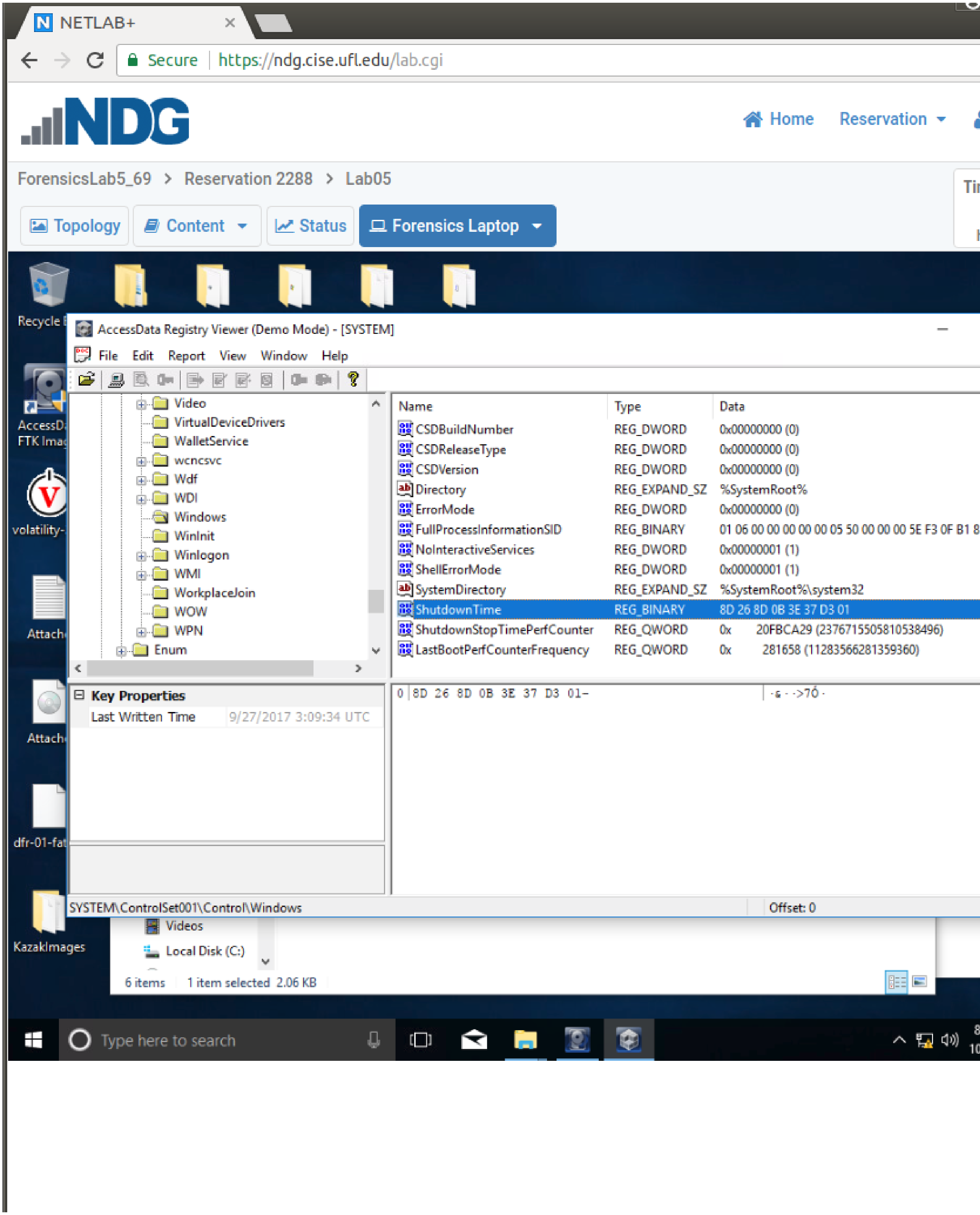
Name	Type	Data
ProfileName	REG_SZ	Maude Wifi 5G
Description	REG_SZ	Maude Wifi 5G
Managed	REG_DWORD	0x00000000 (0)
Category	REG_DWORD	0x00000000 (0)
DateCreated	REG_BINARY	E1 07 08 00 05 00 04 00 0C 00 2E 00 33 00 2B 00
NameType	REG_DWORD	0x00000047 (71)
DateLastConnected	REG_BINARY	E1 07 08 00 05 00 04 00 0C 00 2E 00 33 00 2B 00

Key Properties

Last Written Time	9/27/2017 3:07:37 UTC

```
00  4D 00 61 00 75 00 64 00-65 00 20 00 57 00 69 00  M·a·u·d·e· ·W·i·
10  66 00 69 00 20 00 35 00-47 00 00 00              f·i· ·5·G···
```

SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Profiles\{18751EE5-D736-4873-A29F-1CED273BC325}   Offset: 0



AccessData Registry Viewer (Demo Mode) - [SYSTEM]

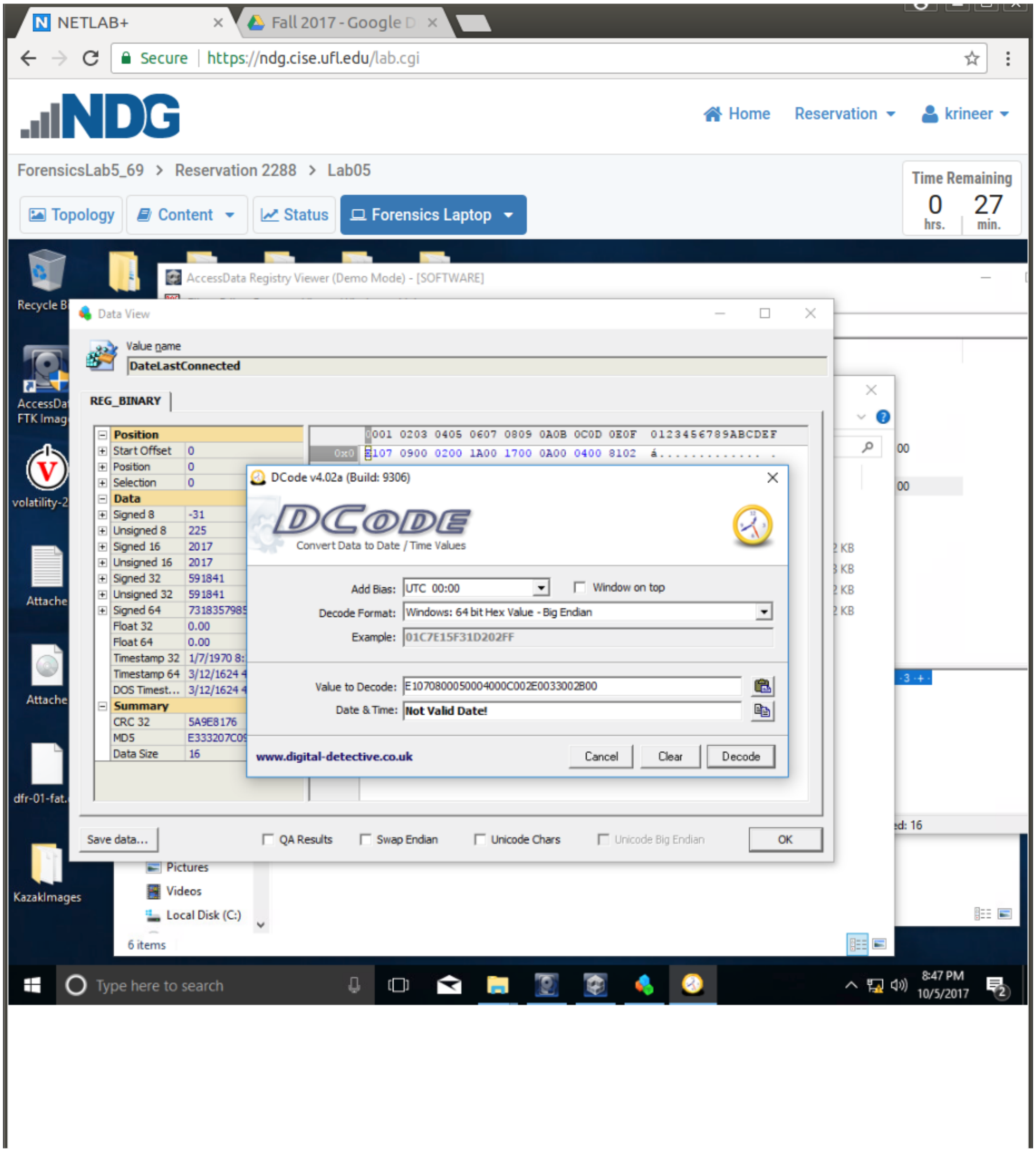
Name	Type	Data
CSDBuildNumber	REG_DWORD	0x00000000 (0)
CSDReleaseType	REG_DWORD	0x00000000 (0)
CSDVersion	REG_DWORD	0x00000000 (0)
Directory	REG_EXPAND_SZ	%SystemRoot%
ErrorMode	REG_DWORD	0x00000000 (0)
FullProcessInformationSID	REG_BINARY	01 06 00 00 00 00 00 05 50 00 00 00 5E F3 0F B1 8
NoInteractiveServices	REG_DWORD	0x00000001 (1)
ShellErrorMode	REG_DWORD	0x00000001 (1)
SystemDirectory	REG_EXPAND_SZ	%SystemRoot%\system32
ShutdownTime	REG_BINARY	8D 26 8D 0B 3E 37 D3 01
ShutdownStopTimePerfCounter	REG_QWORD	0x 20FBCA29 (2376715505810538496)
LastBootPerfCounterFrequency	REG_QWORD	0x 281658 (11283566281359360)

```
0 8D 26 8D 0B 3E 37 D3 01-                    ·ഒ··>7Ó·
```

Key Properties	
Last Written Time	9/27/2017 3:09:34 UTC

SYSTEM\ControlSet001\Control\Windows   Offset: 0

Lab 5 Report
Kevin Rineer
27 Sept 2017



Value name: DateLastConnected

REG_BINARY

Position	
Start Offset	0
Position	0
Selection	0
Data	
Signed 8	-31
Unsigned 8	225
Signed 16	2017
Unsigned 16	2017
Signed 32	591841
Unsigned 32	591841
Signed 64	7318357985
Float 32	0.00
Float 64	0.00
Timestamp 32	1/7/1970 8:
Timestamp 64	3/12/1624 4
DOS Timest...	3/12/1624 4
Summary	
CRC 32	5A9E8176
MD5	E333207C0
Data Size	16

```
     0001 0203 0405 0607 0809 0A0B 0C0D 0E0F  0123456789ABCDEF
0x0  E107 0900 0200 1A00 1700 0A00 0400 8102  á.............. .
```

DCode v4.02a (Build: 9306)

DCODE
Convert Data to Date / Time Values

Add Bias: UTC 00:00 ☐ Window on top
Decode Format: Windows: 64 bit Hex Value - Big Endian
Example: 01C7E15F31D202FF

Value to Decode: E10708000500040000C002E0033002B00
Date & Time: **Not Valid Date!**

www.digital-detective.co.uk

☐ QA Results ☐ Swap Endian ☐ Unicode Chars ☐ Unicode Big Endian